YUCAN

Productinformatie

AVG-Control | Voor scholen & onderwijsinstellingen

SECTOR

Onderwijs

TYPE

Compliance management , Informatiebeveiliging , Informatiemanagement , Privacymanagement , Riskmanagement

BRON

PRODUCTINFORMATIE

AVG-Control | Voor scholen & onderwijsinstellingen

SECTOR

Onderwijs

TYPE

Compliance management , Informatiebeveiliging , Informatiemanagement , Privacymanagement , Riskmanagement

BRON

BESCHRIJVING

Uw eigen online management-omgeving waarin u alles rondom de AVG (incl. IBP) zelfstandig en blijvend organiseert. Inclusief Verwerkingsregister, DPIA's en management van uw verbeter- en beheersingsprocessen. Al uw verantwoordingsdocumenten altijd direct beschikbaar.

GESELECTEERDE MODULES

01. Modules: Evaluatie (looptijd 1 jaar)

PRIJS

€ 339,00 (excl. btw) incl. 25 gebruikers

INHOUDSOPGAVE

1. Informatie

AVG-Control in Yucan (incl IBP)

U start uw eigen online management-omgeving inclusief AVG-Control & IBP.

Met AVG Control in Yucan krijgt u alles rondom de AVG kostenefficiënt en blijvend onder controle. Inhoudelijk èn procesmatig. AVG Control is namelijk een online management-omgeving die u als school in staat stelt om met of zonder consultancy of hulp van derden aan de strenge eisen van de AVG te voldoen.

AVG Control is tegelijk ook uw handleiding voor de AVG! U ziet altijd duidelijk waar u moet beginnen, met op ieder punt uitleg over wat u moet doen en wanneer u moet handelen. Zo heeft u uw volledige AVG-Dossier altijd en blijvend op orde!

U start met of werkt door op de **Aanpak IBP van Kennisnet, PO Raad & VO Raad** Deze is geheel in Yucan beschikbaar en altijd up to date. Inclusief de in het privacy-framework opgenomen checklist IBP.

Van Bewerkingsregister tot kant-en-klare checklists, DPIA's, inbreukregistraties (datalek), privacy-plannen en projectformats: U ziet direct wat u voor de wet (AVG) moet vastleggen en wordt overal waar nodig, door uitleg, voorbeelden en relevante wetgeving ondersteund. En wanneer maar nodig, zijn met één druk op de knop alle verantwoordingsdocumenten beschikbaar.

Start een gratis demo en laat u adviseren!

Start een gratis demo om te zien wat AVG-Control voor u kan betekenen.

AVG-Control biedt u veel en is zeer volledig. Neem daarom **geheel kosteloos** contact op met één van onze adviseurs om uw demo samen te doorlopen. Binnen 10 minuten heeft u een totaal beeld, u ziet direct hoe u alles rondom de AVG doelmatig, zelfstandig en voor 25 Mei organiseert.

Tel: 020 - 5305053

Uw online management-omgeving inclusief

- Aanpak IBP
- Checklist IBP
- Privacy-framework
- Proces-inventarisatie
- Organisatie DPIA's
- Proces DPIA's
- Bewerkingsregister
- Register datalekken
- Privacy beleid & protocollen
- Privacy jaarplan
- AVG-verantwoording
- Beheer & rapportage
- De PDCA rond.

Past dit AVG-Control product bij uw organisatie?

Dit AVG-Control product is geschikt voor middelgrote en grotere scholen; Scholen waar verschillende

verantwoordelijkheden zijn verspreid over meerdere afdelingen of met een duidelijke functiescheiding. Inventarisatie van processen is gegroepeerd op afdelingsniveau. Dit AVG-Control product is met name geschikt voor onderwijsinstellingen / scholen in het VO, VAVO, MBO, HBO en besturen).

- Heeft u een kleine school waar verschillende taken en verantwoordelijkheden bij een beperkt aantal mensen worden ondergebracht en zijn de functies minder gescheiden? Bekijk dan de andere AVG-Control producten.
- Bent u een bedrijf? Of een zorgaanbieder of zorginstelling? Bekijk de AVG-Control producten voor uw sector.

Is de school onderdeel van een bestuurs-structuur?

Formeel juridisch is het bestuur, als de gezaghebbende – als zij degene is die het doel en de middelen bepaalt en aangesproken kan worden op de verwerking – de verantwoordelijke. In die zien kan het bestuur het AVG Dossier voor de afzonderlijke scholen als één geheel beheren.

De praktijk is lastiger: Een bestuur bepaalt mogelijk het doel, de middelen en de regels voor het gebruik van persoonsgegevens. De afzonderlijke school is doorgaans de functionele beheerder van die persoonsgegevens en beslist ook vaak met veel autonomie hoe en met welk doel persoonsgegevens worden gebruikt en ook worden bewaard. Dat kan of zal bij de ene school en de andere school onder een bestuur verschillen. Ook zullen er verwerkingen zijn waar iedere school op zich zijn eigen beslissingen ten aanzien van doel en middelen over neemt. De afzonderlijke school treedt daarbij doorgaans met een eigen herkenbare identiteit naar buiten, waardoor betrokkenen de school als verantwoordelijke zullen zien. Ook al is dat juridisch gezien het bestuur.

- **Advies:** Vanuit de praktijk gezien, is het raadzaam dat de afzonderlijke scholen hun eigen AVG-Dossier bij houden en binnen de bestuurlijke opzet, onderling samenwerking te zoeken voor gemeenschappelijk gebruikte systemen en afspraken. Ook voor de werkbaarheid en beheersbaarheid een surplus, want iedere school kan zo zijn eigen deel bijhouden.
- **Verantwoording:** Scholen kunnen zich autonoom bewegen en apart verantwoorden. Indien de AP het bestuur vraagt om verantwoording kunnen AVG-Dossiers in Yucan eenvoudig worden samengevoegd.

Bekijk de inhoud

Een deelweergave van uw AVG-Proces, Aanpak IBP, behulpzame uitleg, procesinventarisatie, checklist IBP, privacy framework, en wetgeving (AVG) heeft u direct in beeld.

De werking en inhoud van verwerkingsregister, DPIA's, behandellijst, verbeter- en privacy plannen en rapportagevormen ziet u in de demo in de module 'ontwikkelen'.

Bekijk de inhoud via de betreffende tab hierboven of start een demo om verder te kijken.

Werkwijze & looptijd kiezen

Kies een werkwijze door onder de tab 'Modules en proces' een combinatie van modules te kiezen. U kunt compact beginnen en altijd uitbreiden naar een team-aanpak. U ziet daar het gekozen proces en of deze het beste bij uw doelstellingen past. U leest in het kort wat u in de verschillende modules kunt doen en wat uw output is.

Let op!

- U kunt nu ook een **maandlicentie** nemen om eerst eens te kijken waar u staat en verbeterpunten vaststellen! Wilt u daarbij ook registraties doen en DPIA's uitvoeren?
- **> Kies dan voor een werkwijze met ontwikkelmodule.**

- En wilt u uw DPIA's en verwerkingsregister buiten Yucan uitvoeren en beheren? Maar wel werken met de Aanpak IBP, de checklist, procesinventarisatie en het privacy framework?
- > Kies dan voor een werkwijze **zonder** ontwikkelmodule. U kunt deze later altijd toevoegen.

Uw proces (PDCA) in AVG-Control ziet er als volgt uit:

Stap 1 Inventariseren & Beheren(evaluatiemodule)

U werkt o.b.v. de Aanpak IBP, aangevuld met de checklist IBP in het privacy-framework. U inventariseert en brengt de processen waar persoonsgegevens worden gebruikt in kaart. Zo weet u zeker dat u niets over het hoofd ziet. Samen met de analyse in het Privacy Framework heeft u uw Organisatie DPIA in de basis op orde.

Stap 2 Analyseren, Vastleggen & Prioriteren (ontwikkelmodule)

Hier legt u alle bewerkingen vast die automatisch in het Bewerkingsregister komen. Daarbij checkt u o.a. of verwerking wetmatig is en direct ook of een DPIA vereist is. Voert u die DPIA ook uit dan brengt u eventuele verbeterpunten ook direct in beeld. AVG control genereert automatisch een overzichtelijke behandellijst.

Stap 3 Documenteren, Verbeteren & Plannen (ontwikkelmodule)

Hier documenteert u uw privacybeleid, datalekken, protocollen, handboeken en privacy (jaar)plannen. En met behulp van de handzame en flexibele formats in AVG Control werkt u hier al uw verbeterprojecten uit.

Stap 4 Overzicht, bewerkingsregister & Verantwoording (ontwikkelmodule)

AVG Control is zo opgezet dat u continu een samenhangend overzicht heeft èn houdt van alle processen, bewerkingen, incidenten, beschrijvingen, verbeterprojecten & privacyplannen. En met één druk de knop heeft u al uw rapportages en verantwoordingsdocumenten altijd direct beschikbaar.

Rapportage en verantwoording AVG

Alles geintegreerd en direct beschikbaar voor de vereiste verantwoordingswijze van de toezichthouder (AP).

Met een druk op de knop heeft u op ieder gewenst moment de beschikking over allerhande keurig verzorgde rapportages (scherm en pdf). Van de uitkomsten uit uw inventarisatie tot volledige DPIA's. Uw complete verwerkingsregister t/m behandellijsten, verbeterprojecten en privacyplannen.

Binnen uw account werken met meerdere producten en werkomgevingen

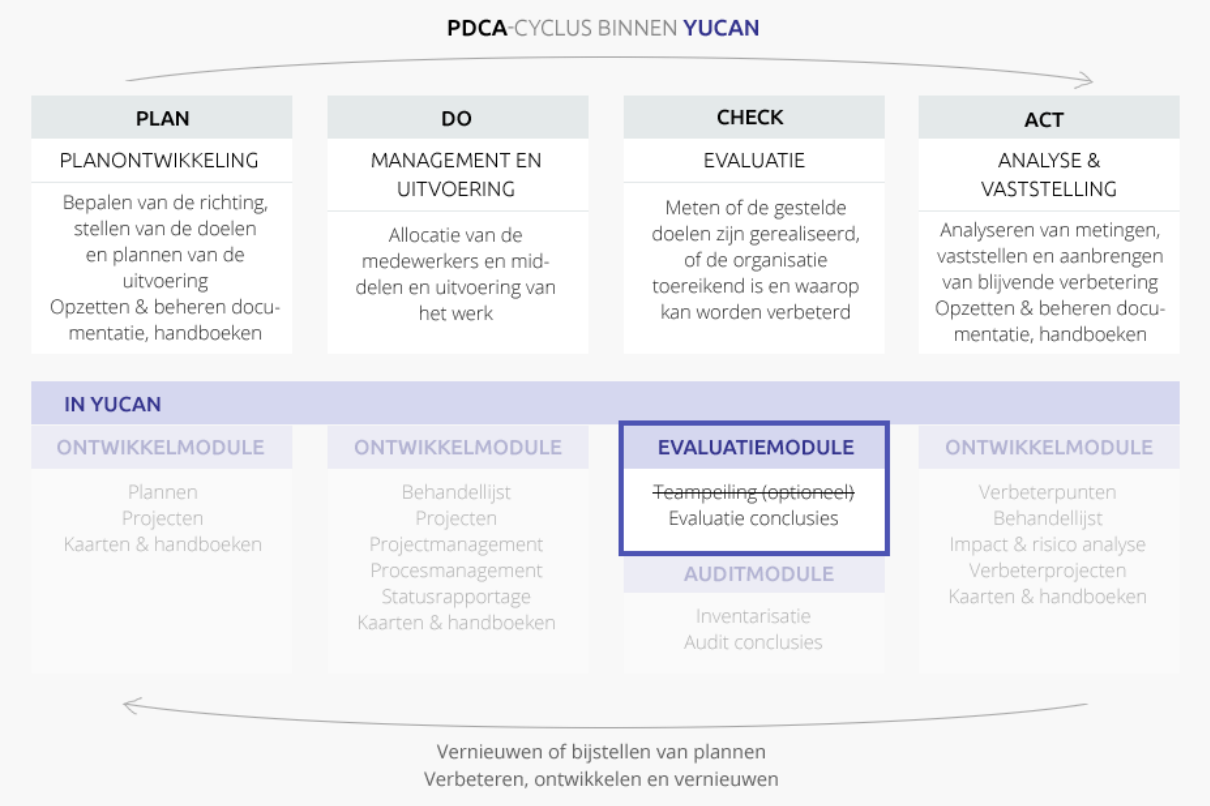
Heeft u al een account? Binnen uw account kunt u voor het werken met iedere afzonderlijk product steeds een eigen werkruimte activeren. Dus ook voor uw AVG-Control. Zo heeft u alles goed georganiseerd.

U kunt er voor kiezen binnen één werkruimte samen te werken o.b.v. een product. Ook kunt u voor ieder afzonderlijk deel van uw organisatie een eigen werkruimte met het betreffende product activeren. Per werkruimte of door meerdere werkruimten te activeren kunt u andere betrokkenen

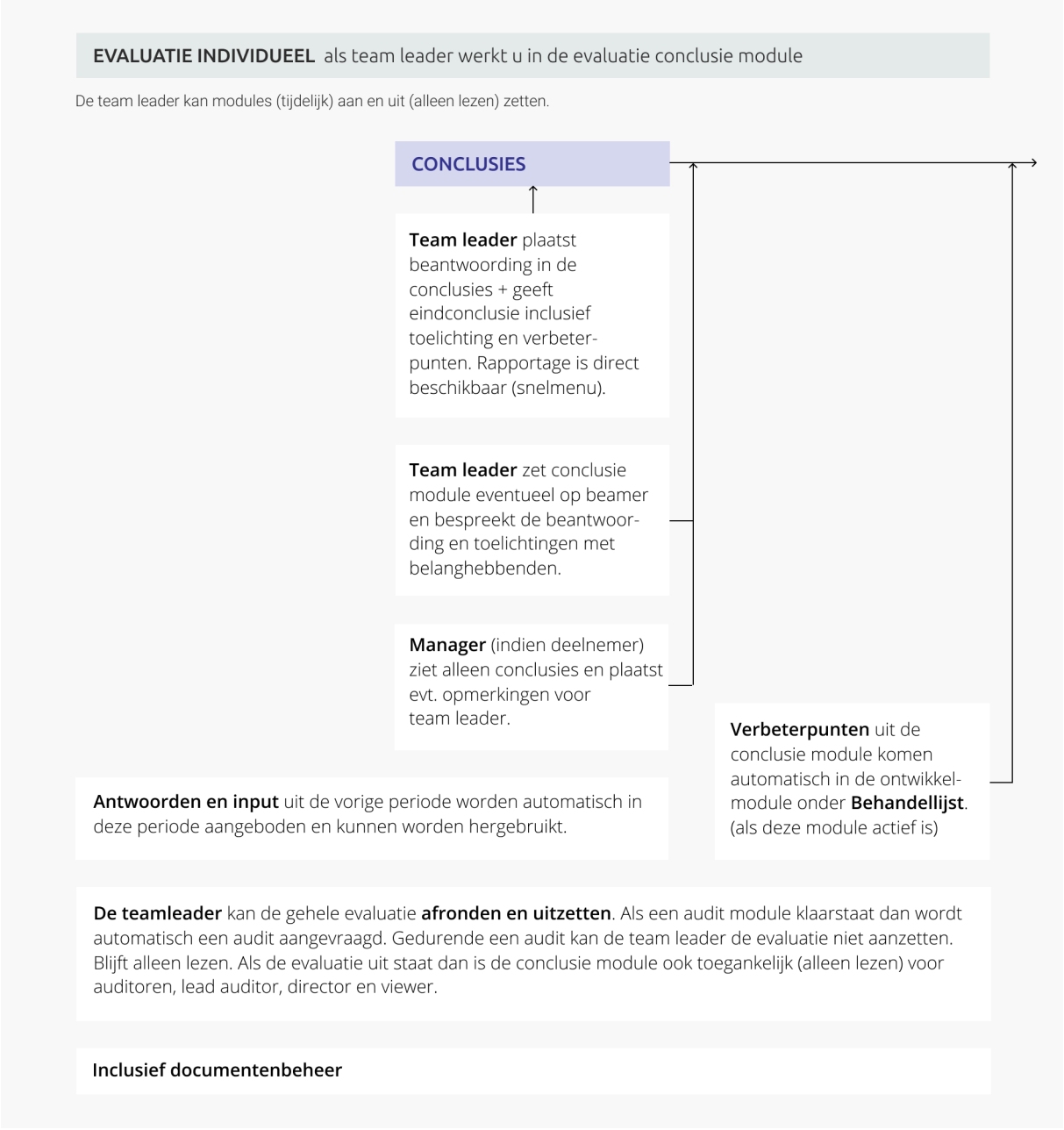
aanwijzen en het beheer en de opvolging in uw organisatie spreiden. U en uw collega's kunnen gelijktijdig bij meerdere werkruimten betrokken zijn terwijl de regie centraal kan blijven.

2. Modules en proces

Proces in beeld



Evaluatie individueel



Evaluatie - Conclusie

U evalueert de in het portfolio aangeboden onderwerpen. U beantwoordt de vragen, geeft eventueel toelichtingen en benoemd verbeterpunten. Zo nodig voegt u per onderwerp onderbouwende documenten (bewijsstukken) toe. Conclusies uit een eventuele eerdere periode of (teamevaluatie) input van deelnemers aan de peiling kunt u met een druk op de knop kopiëren. Door u benoemde verbeterpunten worden - indien de ontwikkelmodule wordt gebruikt - ook automatisch in uw behandellijst getoond.

U hebt de beschikking over uitgebreide rapportage van uw conclusies. Heeft u meerdere portfolio's? Dan kunt u de gegevens in rapporten combineren. Uw gegevens blijven bewaard en kunnen in een volgende periode eenvoudig worden hergebruikt.

3. Inhoud

AVG-Control incl IBP - Voor middelgrote en grote scholen / onderwijsinstellingen (zoals: VO, VAVO, MBO, besturen)

I. Proces en PDCA in beeld

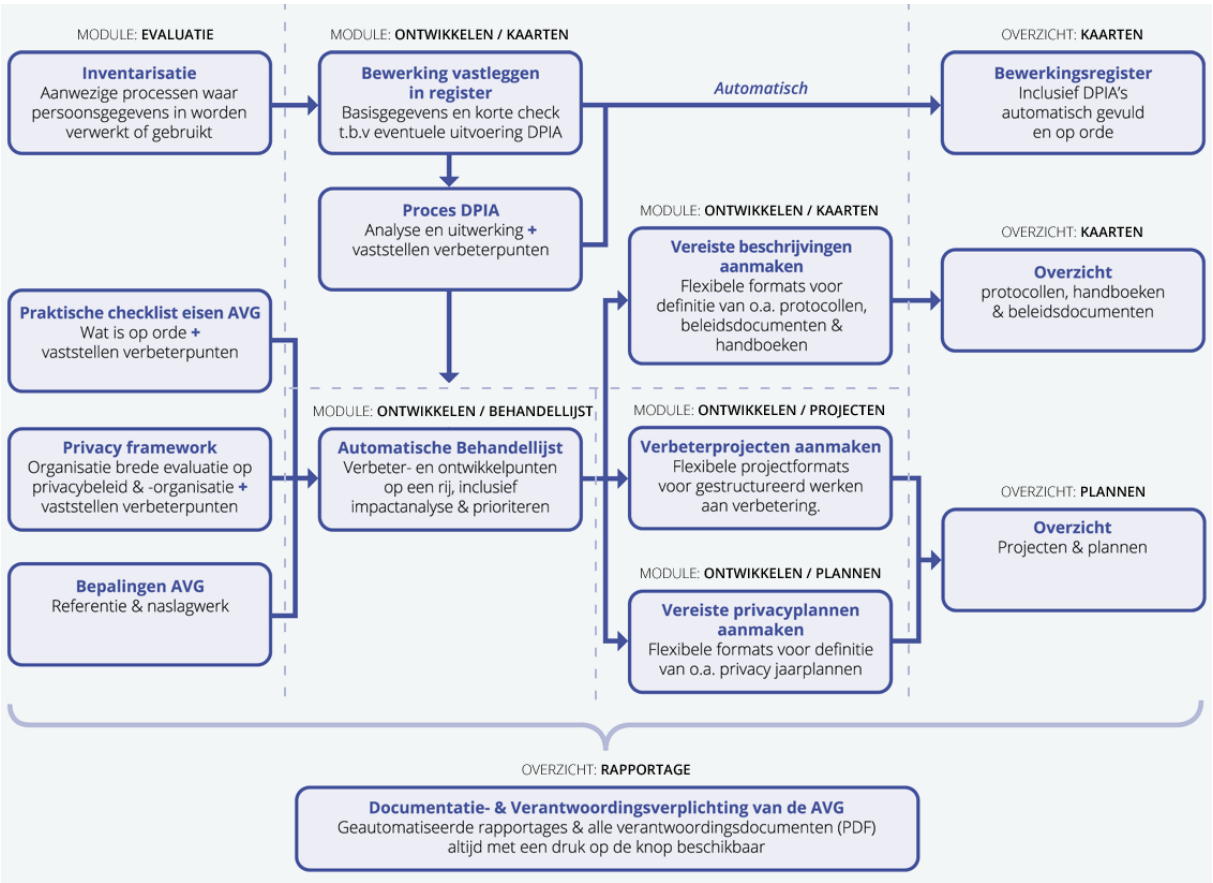
I. Proces en PDCA in beeld

AVG Control werkt intuïtief. U ziet altijd duidelijk waar u moet beginnen, wat u moet doen en wanneer u moet handelen. Van Bewerkingsregister tot organisatiebrede checklist (Privacy framework), DPIA's, privacy-plannen en projectformats: alles is helder vormgegeven en wordt overal waar nodig, door uitleg, voorbeelden en relevante wetgeving ondersteund. En wanneer maar nodig, zijn met één druk op de knop alle verantwoordingsdocumenten beschikbaar.

In 4 stappen blijven 'in control'

Via onderstaand schema ziet u direct welke stappen u waar in Yucan/AVG-Control doet.

U kunt alles op ieder moment benaderen en gebruiken. Uw ideale route is van links naar rechts.



Stap 1 Inventariseren & Beheren

In het privacy-framework evalueert u waar u staat. Met de proces inventarisatie brengt u de processen waar persoonsgegevens worden gebruikt in kaart. Zo weet u zeker dat u niets over het hoofd ziet. En zo heeft en houdt u uw Organisatie DPIA volledig op orde.

Stap 2 Analyseren, Vastleggen & Prioriteren

U legt alle bewerkingen vast die automatisch in het Bewerkingsregister komen. Daarbij checkt u meteen of een DPIA vereist is. Voert u die DPIA ook uit dan brengt u eventuele verbeterpunten ook direct in beeld. AVG control genereert automatisch een overzichtelijke behandellijst.

Stap 3 Documenteren, Verbeteren & Plannen

Hier documenteert u uw privacybeleid, protocollen, handboeken en privacy (jaar)plannen. En met behulp van de handzame en flexibele formats in AVG Control werkt u hier al uw verbeterprojecten uit.

Stap 4 Overzichten, bewerkingsregister & Verantwoording

AVG Control is zo opgezet dat u continu een samenhangend overzicht heeft èn houdt van alle processen, bewerkingen, beschrijvingen, verbeterprojecten & privacyplannen. En met één druk de knop heeft u al uw rapportages en verantwoordingsdocumenten altijd direct beschikbaar.

II. Aanpak IBP Kennisnet - PO Raad - VO Raad

Welkom bij de online 'aanpak informatiebeveiliging en privacy'!

Deze aanpak is ontwikkeld door Kennisnet, PO Raad en VO Raad voor scholen in het primair en voortgezet onderwijs, zodat mensen zonder achtergrondkennis over deze onderwerpen hier toch invulling aan kunnen geven. Zij hebben de nodige kennis en expertise vertaald naar het onderwijs. Lekker. Eenvoudig.

De rol van Kennisnet

Iedere school is uniek. Maar daarmee is niet iedere aanpak voor informatiebeveiliging en privacy uniek. Er zijn nu eenmaal zaken die je op elke school geregeld moet hebben. Het lijkt een berg werk, maar je kan IBP stap voor stap regelen.

Kennisnet heeft met eigen expertise en veel bezoeken aan scholen bekeken wat werkt en wat veel voorkomende uitdagingen zijn. Eén van de dingen die altijd werkt is een eenvoudige uitleg zoeken zodat je met elkaar het gesprek over IBP aan kan gaan.

Dat is dan ook het uitgangspunt geweest voor de PO-Raad, VO-raad en Kennisnet om een aanpak te ontwikkelen die scholen helpt met het op eenvoudige en praktische wijze organiseren van informatiebeveiliging en privacy (IBP). Deze aanpak draagt er aan bij dat de privacy van leerlingen en medewerkers is gegarandeerd, terwijl de continuïteit van het onderwijs geregeld is. Scholen zijn daarmee in staat om in de toekomst eigentijds, veilig en persoonlijk onderwijs te blijven geven met behulp van ict.

Deze aanpak wordt pas écht van het onderwijs als Kennisnet van jou te horen krijgt wat je ervan vindt. En waar je aanvullend behoefte aan hebt. Yucan en AVG Control vullen de IBP aan op basis van de aanvullingen die Kennisnet doorvoert. Zo maken we het onderwijs samen een stuk veiliger.

Voor vragen, opmerkingen of ideeën m.b.t. de IBP kun je contact opnemen met de IBP-helpdesk via ibp@kennisnet.nl of 0800-3212233

Aanpak IBP voor het PO en VO
Auteur: Kennisnet, PO Raad, VO Raad
Laatst gewijzigd 18 december 2017

Webadres https://maken.wikiwijs.nl/81891

De rol van Yucan en AVG Control

Yucan biedt de IBP van Kennisnet PO Raad VO Raad aan binnen AVG Control producten voor PO en VO. Met als doel volledig en behulpzaam te kunnen zijn op het gebied van privacy managament. Yucan biedt met AVG Control een online werkruimte en AVG Dossier waar alle processen rondom de AVG en dus ook de IBP eenvoudig, goed en betaalbaar door onderwijsinstellingen kunnen worden georganiseerd en beheerd. De combinatie van IBP binnen de AVG producten in Yucan ligt daarom voor de hand.

- Via de proces-inventarisatie brengt u uw processen en verwerkingen op een gemakkelijke manier in beeld. U houdt ze goed geordend bij elkaar om altijd beeld te hebben
- Vervolgens registreert u ze in het verwerkingsregister in Yucan en zo nodig voert u een risicoanalyse (PIA) uit. Incl. checks op o.a. rechtmatigheid verwerking.
- Alle onderwerpen uit de IBP en de vereisten van de AVG komen sluitend en in detail aan de orde in het privacy-framework.
- Zo hebt u altijd een eindcontrole op de wet en een totaalbeeld van waar u staat.

De downloads in de IBP staan ook in de bibliotheek van uw werkruimte om op ieder gewenst moment bij de hand te hebben.

Binnen de onderdelen van de IBP waar een activiteit of actie wordt voorgesteld, biedt Yucan steeds de ruimte om aan te geven wat de activiteit of actie is die u ter hand neemt. U gebruikt daarvoor dan de in Yucan aanwezige formats voor:

- registraties,
- PIA's,
- protocollen,
- procesbeschrijviingen,
- privacy-dcoumenten en
- verbeterplannen.

En natuurlijk kunt u deze ook als losse documenten toevoegen.

Daarbij kunt u steeds aangeven wat daarvan de status is en welke verbeterpunten u ziet. Op die manier houdt u al uw privacybeheer en -activiteiten duurzaam onder controle. En heeft u al uw verantwoordingsdocumenten met een druk op de knop beschikbaar.

In het Privacy-framework heeft u een checklist IBP tot uw beschikking om te kunnen kijken of u invulling hebt kunnen geven aan de aangeboden onderwerpen. Voor een verdere check op de AVG; Doorloop het privacy-framework.

Zo werkt de Aanpak IBP

Deze online aanpak is ontwikkeld voor jou als bestuurder, docent, ict-coördinator of communicatiemedewerker op een school. Vaak is IBP maar één van de onderwerpen waar je mee bezig bent en kun je er niet je volle werkweek aan besteden. De Aanpak helpt je IBP goed te regelen met voorbeelddocumenten, uitleg en praktische tips in drie eenvoudige stappen:

Hoofdstuk 1: Organiseren

In de eerste stap helpen we je met tips en voorbeeldteksten om eenvoudig een eerste IBP-beleid voor jouw school te maken. Je krijgt twee voorbeelden van een beleid, die inhoudelijk dezelfde onderdelen bevatten. We geven een aantal aandachtspunten en stellen een document beschikbaar waarin we elke
stap toelichten. Je kunt ook je bestaande beleid aanscherpen op basis van de voorbeelden.

Hoofdstuk 2: Realiseren

Maar wat ga je nu in de dagelijkse praktijk doen? In de tweede stap wordt het beleid gerealiseerd door het nemen en plannen van de nodige technische en juridische maatregelen en activiteiten. We helpenje met een uitleg, voorbeelden, checklists en handige bronnen.

Hoofdstuk 3:Communiceren

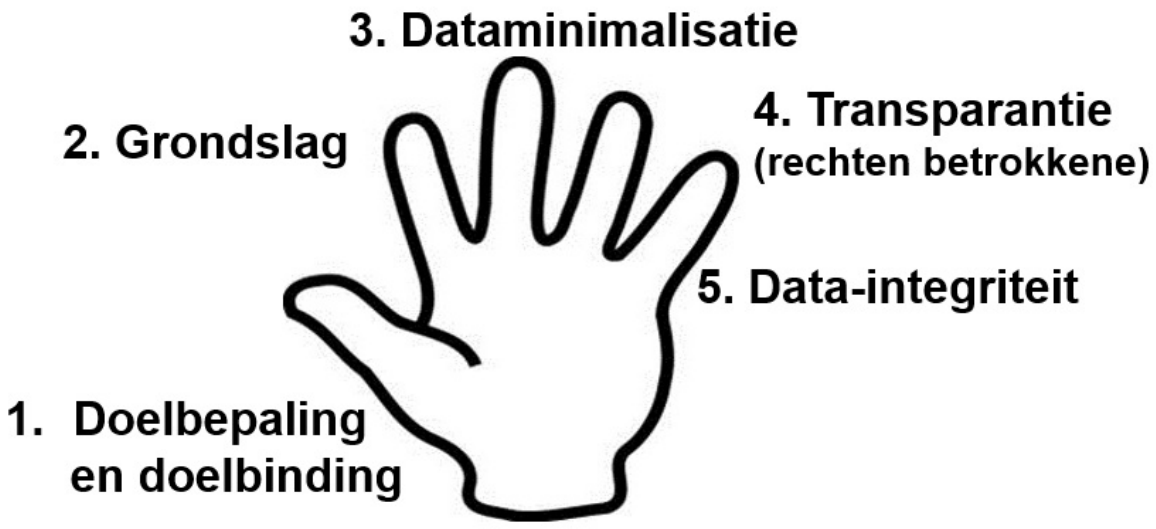
Een belangrijk onderdeel van IBP is het duidelijk communiceren naar alle belanghebbenden. Dit laatste hoofdstuk geeft je tips en trucs hoe je dit het beste kunt aanpakken.

Doorloop je de aanpak stap voor stap, dan kom je alles tegen wat je moet regelen. Je kan niet alles in één keer uitvoeren. Daarom zullen we ook duidelijk aangeven wat je op korte termijn moet doen en wat je later kan plannen.

We raden je aan om eerst de hele aanpak te doorlopen. Dan heb je een goed en compleet beeld. Is alles nieuw voor je? Begin dan gewoon met 'Organiseren'. Klinken veel zaken bekend, dan kun je links zelf de voor jou relevante onderwerpen uit de aanpak uitkiezen.

Basisbegrippen IBP

Het is belangrijk om een aantal basisregels te kennen vanuit de privacy wetgeving. Deze basisregels komen voort uit de Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018) en de Algemene Verordening Gegevensbescherming (AVG; na 25 mei 2018). Kennisnet heeft de belangrijkste uitgangsprincipes voor privacy als 5 vuistregels weergegeven.



Naast deze vijf vuistregels voor het gebruik van persoonsgegevens zijn er een aantal begrippen die je moet kennen als je IBP op school goed wilt regelen. Deze zijn in het onderstaande document '*privacy - dit moet je weten over de wet*' uitgewerkt samen met een uitleg over de 5 vuistregels.

Aandachtspunten AVG mei 2018

Het Europees parlement stemde in 2016 in met de **Algemene Verordening Gegevensbescherming** (AVG). Deze nieuwe wetgeving sluit aan op technologische ontwikkelingen en globalisering. Door de AVG zijn persoonsgegevens van alle EU-inwoners straks op dezelfde wijze beschermd, ongeacht of hun gegevens zijn opgeslagen in Europa of - bijvoorbeeld - de Verenigde Staten.

Dat betekent dat er vanaf 25 mei 2018 nog maar één privacywet geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer. De AVG is een verordening, dit houdt in dat er rechtstreeks verplichtingen worden opgelegd aan degene die persoonsgegevens verwerken en rechten toekent aan betrokkenen (degene van wie persoonsgegevens verwerkt worden). Ook Nederlandse scholen moeten vanaf 25 mei 2018 voldoen aan de nieuwe wetgeving. Dat betekent huiswerk voor scholen die privacy nog niet goed hebben geregeld.

Als de Algemene Verordening Gegevensbescherming (AVG) van toepassing is, hebben organisaties die persoonsgegevens verwerken meer verplichtingen. Er wordt in de AVG meer nadruk gelegd op de verantwoordelijkheid van organisaties (scholen) zelf. Scholen moeten niet alleen de **wet naleven**, zij moeten kunnen **aantonen** dat zij zich aan de wet houden.

De volgende 10 onderwerpen laten niet alleen de uitbreidingen en aanpassingen van de huidige regels van de Wbp zien, maar bevatten ook de nieuwe elementen die zijn toegevoegd in de AVG.

- Uitgangspunten privacy (5 vuistregels2.0)
- Privacy by design / by default
- Verplichte risicoanalyse
- Documentatieplicht
- Bewustzijn creëren en voorlichten
- Gebruik digitale diensten onder de 16 jaar
- Bewerkersovereenkomsten
- Meldplicht datalekken
- Functionaris voor Gegevensbescherming
- Technische en organisatorische maatregelen

Maar wat betekent dit voor mijn school, mijn organisatie? Lees hierover meer in het volgende document:

1. Organiseren

In de eerste stap helpen we je met tips en voorbeeldteksten om eenvoudig een eerste IBP-beleid voor jouw school te maken. Je krijgt twee voorbeelden van een beleid, die inhoudelijk dezelfde onderdelen bevatten. We geven een aantal aandachtspunten en stellen een document beschikbaar waarin we elke
stap toelichten. Je kunt ook je bestaande beleid aanscherpen op basis van de voorbeelden.

Waarom heb ik een beleidsplan nodig?

We hebben gezien dat wetgeving niet alleen bepaalt onder welke voorwaarden persoonsgegevens gebruikt mogen worden, maar ook aangeeft dat er passende technische en organisatorische maatregelen genomen moeten worden om de persoonsgegevens te beschermen.

Om hieraan te voldoen zal een school dan ook moeten vastleggen wat er wel en niet met persoonsgegevens gedaan mag worden. Als school moet je weten waar de risico's liggen en wat je eraan kan doen.

Het gaat in eerste instantie niet om die technische maatregelen, niet om ict, maar om gedrag, cultuur en bewustwording. IBP is geen techniek feestje, het is een constant bewustzijn van de risico's die een

school loopt. Niet alleen risico's waardoor de continuïteit in zowel het onderwijs als de bedrijfsvoering in gevaar kan komen, maar ook risico's rondom het beschermen van de privacy van leerlingen en medewerkers. Het IBP-beleid, met de onderliggende afspraken, procedures en verantwoordelijkheden moet school-breed geïmplementeerd zijn, dan pas is ict aan zet bij de 'technische' uitvoer en monitoring.

Het schoolbestuur is verantwoordelijk om informatiebeveiliging en privacy (IBP) te regelen. Het regelen van IBP begint dan ook met een goedgekeurd en bij iedereen bekend gemaakt IBP-beleid. Dat is de basis, de kapstok, om processen, richtlijnen en procedures rondom IBP uit te werken.

Maar wat moet je nu als bestuurder zelf doen en wat kan je bij anderen neerleggen?

- Van belang is dat je als bestuurder de organisatie rondom IBP goed inricht.
- De basisbegrippen IBP en de aandachtspunten AVG geven een bestuurder belangrijke informatie om IBP goed te regelen.
- Als bestuurder laat je IBP ook regelmatig op de agenda terugkomen. Het is belangrijk om op basis van rapportages en nieuwe ontwikkelingen IBP te evalueren.

IBP is een soort **vliegwiel** wat je op gang moet brengen.

Dat betekent grosso modo de volgende inspanning voor het eerste half jaar:

▪ Eén persoon toegewijd aan IBP	1 á 2 dagen per week
▪ Actieve betrokkenheid van het bevoegd gezag	1 dag per maand
▪ ICT (maatregelen inventariseren en nemen)	8 dagen per maand
▪ HR, administratie (maatregelen nemen)	4 dagen per maand

Daarna, wanneer het proces eenmaal loopt:

▪ Eén persoon toegewijd aan IBP	0,5 dag per week
▪ Actieve betrokkenheid van het bevoegd gezag	1 dag per kwartaal
▪ ICT (maatregelen controleren en nemen)	2 dagen per maand
▪ HR, administratie (maatregelen nemen)	1 dag per maand

LET op: dit zijn inschattingen van dit moment en kunnen per organisatie verschillen. Dit is o.a. afhankelijk van de grootte van de organisatie.

Hoe maak je een beleidsplan?

Scholen hebben soms een andere insteek voor het beleid. De ene school wil beleid makkelijk kunnen communiceren met medewerkers. De andere school wil het beleid formeel vastleggen voor compliance. Hou bij beide in het achterhoofd dat het beleid de basis is, de kapstok, om processen, richtlijnen en procedures rondom IBP verder uit te werken en vast te leggen.

Het is belangrijk om te beseffen dat je eerste IBP-beleid een vertrekpunt is. Het kan goed zijn dat in de loop van de tijd veranderingen in de techniek, de situatie op school of wijzigingen in wet-en regelgeving vragen om aanpassing van het beleid.

Dit is dan ook de aanleiding geweest om het format IBP-beleid aan te passen aan de AVG. In het nieuwe format is rekening gehouden met o.a. rechten van betrokkenen, de verplichting om vast te leggen welke persoonsgegevens verwerkt worden (dataregister), de (D)PIA, privacy by design en privacy by default, de functionaris voor gegevensbescherming en meer.

Let op: Vanuit de AVG gaat het er niet alleen om dat scholen de wet**naleven**, zij moeten ook kunnen **aantonen** dat zij zich aan de wet houden. Dit is van belang zijn als je het beleid verder gaat uitwerken.

Templates (deze staan ook in uw bibliotheek in Yucan)

Ook nu gaan we uit van twee templates als voorbeeld. In beide templates vind je een volledige hoofdstukstructuur, voorbeeldteksten en 'gele velden' velden. De opzet is dus hetzelfde, alleen het taalgebruik is anders.

De formele versie is voorzien van een extra document met dezelfde inhoud, en een extra kolom met een aparte toelichting. Deze toelichting bevat verdere uitleg en verwijzigingen naar onderliggende documenten, afspraken en procedures. Hiermee wordt de 'kapstokfunctie' van het beleid inzichtelijker. Het laat enerzijds zien wat de achterliggende gedachte is van bepaalde afspraken, maatregelen en procedures en anderzijds geeft het je de mogelijkheid om aantoonbaar te maken dat je aan bepaalde vereisten vanuit de AVG voldoet.

Als je een vliegende start wilt maken, hoef je alleen de 'gele' velden in te vullen zodanig dat deze voor jouw schoolorganisatie passend zijn. Daarmee heb je de eerste versie van het IBP-beleid om intern te bespreken en goed te (laten) keuren. Begin je liever met een schone lei, of heb je al een IBP-beleid? Ook goed! Zorg dan in ieder geval dat alle onderwerpen die in het template staan ook in je eigen IBP-beleid terugkomen.

We hebben gemerkt dat het onderdeel **Organisatie** uit het beleid een lastig stuk is. De vraag ‘wie doet wat’ invullen en dus de verantwoordelijkheden goed beleggen is niet voor alle scholen zo eenvoudig. Daarom gaan we daar apart aandacht besteden in het volgende blok.

Wie doet wat?

Ondanks dat iedere school anders georganiseerd is, kom je veelal dezelfde functies, rollen en taken tegen. Dat geldt ook voor het organiseren van IBP. In dit onderdeel helpen we je om de juiste rol- en taakverdeling voor IBP in je beleid op te nemen.

Bedenk hierbij vooral:

- *Wie gaat er verantwoordelijk zijn voor een bepaalde taak?*
- *Waar gaat het precies over? Denk hierbij aan afspraken, processen en dagelijks werk.*
- *Welke documenten (of andere manieren van vastlegging) ondersteunen dit?*

Probeer rollen en taken zo specifiek mogelijk te omschrijven. Dit maakt de afspraken binnen de school duidelijk voor iedereen. In de tabel IBP rollen en taken (zie download verderop) hebben we vast een opzet gemaakt.

De kolom **‘wie’** geeft aan welke rol de genoemde verantwoordelijkheden/ taken op zich kan nemen.

- Op **strategisch niveau** is de bestuurder verantwoordelijk om IBP goed te regelen en daarmee ook om de IBP organisatie goed in te richten. Kies de benaming die het best bij de organisatie past.
- Een **manager informatiebeveiliging en privacy** (afgekort als manager IBP) is een rol op strategisch, tactisch en operationeel niveau. Hij/zij adviseert o.a. de bestuurder. De manager IBP bewaakt de uniformiteit op het gebied van IBP binnen de instelling. Het kan een fulltime rol zijn of een rol die iemand erbij krijgt, dat hangt af van de grootte van de organisatie. Het gaat er niet om dat er extra rollen en/of functies gemaakt moeten worden, maar dat gekeken wordt wie op jou school die taken kan vervullen. Ook kan één persoon prima meerdere rollen vervullen. Let daarbij wel op dat de rollen niet conflicteren met andere verantwoordelijkheden. Kies ook hier de benaming die het best bij de organisatie past.
- Een **proces eigenaar** is iemand die verantwoordelijk is voor één van de primaire of ondersteunende processen, zoals HRM/P&O, administratie, financiën of onderwijs.

In de kolom **‘hoe’** staat aangegeven welke verantwoordelijkheden en taken er minimaal belegd moeten worden. Kijk hierbij goed naar de inhoud van de taken en de werkzaamheden die daarbij horen. Zijn dat éénmalige activiteiten of komen ze zeer regelmatig terug. Een rol als manager IBP kun

je niet 'zomaar even tussendoor' doen. De tijd die het vraagt is mede afhankelijk van de grootte van je organisatie.

De kolom **'wat'** geeft de praktische uitwerking van het beleid op elk niveau weer. Welke processen worden er door wie beschreven, wie legt welke afspraken vast, wie keurt deze goed en hoe wordt er gecommuniceerd.

Een schematische weergave kan helpen de juiste verdeling te maken op strategisch, tactisch en operationeel niveau. Zie de download verderop.

Extra aandacht vragen de volgende punten:

Toegang en toegangsbeleid

- Het is voor informatiebeveiliging en privacy héél belangrijk om te weten wie waar bij mag en wie daarover uiteindelijk de beslissingen neemt. Daarom is het goed om iemand specifiek hiervoor verantwoordelijk te maken.

Individuele medewerkers

- Degene die het meest in aanraking komen met persoonsgegeven, zijn de medewerkers. Docenten leggen veel gegevens van leerlingen vast om ze op de juiste manier te kunnen begeleiden en ook administraties verwerken veel persoonsgegevens. Het is daarom belangrijk dat alle medewerkers het belang van informatiebeveiliging en privacy inzien en erkennen. Betrek hen dan ook zoveel mogelijk bij het hele proces.

Van plan naar uitvoering

Het goedgekeurde IBP-beleid is er.... Maar hoe nu verder? Het is belangrijk dat dit geen papieren tijger wordt of stof gaat staan vangen in de kast. De bedoeling is dat dit beleid in het DNA van alle medewerkers komt te zitten en dat het geheel regelmatig geëvalueerd en zo nodig aangepast wordt.

Communicatie: Zorg dat iedereen bekend is met het IBP beleid

het lezen formaliseren

- Het is belangrijk dat iedereen die bij de school komt werken ook weet wat de 'huisregels' zijn. Dit kan een reden zijn om het lezen van het IBP-beleid en de onderliggende afspraken onderdeel te maken van de arbeidsvoorwaarden. Tekent een nieuwe medewerker voor de arbeidsvoorwaarden, dan geeft dat aan dat deze het IBP-beleid, en de onderliggende afspraken heeft gelezen en de consequenties ervan begrepen heeft. Voor externen kan het op dezelfde manier geregeld worden, door het in de contractvoorwaarden op te nemen.

het lezen stimuleren

- Maar je hebt natuurlijk ook bestaande medewerkers, hoe bereik je die? Enkele tips hiervoor zijn:

- Creëer urgentie door op de volgende teamvergadering voorbeelden te tonen wat er fout kan gaan als je IBP niet goed regelt. Voorbeelden hiervan zijn datalekken die nu (te) vaak in het nieuws komen.
- Gebruik de kracht van de herhaling. Het eenmalig in een vergadering noemen van de term 'IBP' is voor de meeste mensen te weinig. Benoem het belang van IBP in nieuwsbrieven, breng het regelmatig ter sprake tijdens bijeenkomsten.

extra aandacht besteden aan bewustwording

- Hiervoor verwijzen we vast naar hoofdstuk 3; het onderdeel communiceren medewerkers, waar twee mogelijkheden gegeven worden om bewustwording binnen je school onder de aandacht te brengen.

Evalueer regelmatig; IBP is een continue proces

Als je wilt kunnen zeggen dat je IBP onder controle hebt, dan moet je dat kunnen aantonen. Maar hoe weet je of je het onder controle hebt? Door regelmatig te evalueren komen de punten naar voren, die verbetering en/of aanpassing vragen. Nieuwe ontwikkelingen zoals nieuwe processen of nieuwe systemen, maar ook nieuwe wet-en regelgeving kunnen om aanpassingen vragen.

In onderdeel C over evalueren en verbeteren lees hoe je dat kunt regelen.

2. Realiseren

Maar wat ga je nu in de dagelijkse praktijk doen? In de tweede stap wordt het beleid gerealiseerd door het nemen en plannen van de nodige technische en juridische maatregelen en activiteiten. We helpenje met een uitleg, voorbeelden, checklists en handige bronnen.

Start

Nu het beleid op papier staat, moeten we zorgen dat er verdere invulling aan gegeven wordt. In deze module maken we daar een start mee. We gaan **maatregelen** nemen, procedures uitwerken en nog veel meer. Hiervoor is het belangrijk dat we weten op welke **gebieden** IBP een rolt speelt en waar de risico's liggen.

Achtergrond van de maatregelen

De maatregelen die we kunnen en soms moeten nemen zijn gebaseerd op:

- **De code voor Informatiebeveiliging (ISO 27001 / 27002);** deze beschrijft welke beveiligingsmaatregelen van een instelling (mogen) worden verwacht om informatie goed te beveiligen;
- het daarvan afgeleide **normenkader voor HBO en MBO,** dat ook voor het PO en VO op veel punten bruikbaar is*;
- richtlijnen en uitgangspunten die zijn gebaseerd op de huidige **relevante wet- en regelgeving**, waaronder de Algemene Verordening Gegevensbescherming (AVG) en de meldplicht datalekken;
- de in het onderwijs **toegepaste standaarden** (waaronder 'ROSA katern IBP').

Al deze normen en standaarden geven aan welke maatregelen van een school worden verwacht op het gebied van informatiebeveiliging en privacy. Als je ze allemaal moet lezen, begrijpen en moet toepassen in jouw school dan is dat veel werk. Daarom is in deze aanpak IBP de essentie er voor je uit gehaald.

**Bij het Normenkader informatiebeveiliging MBO hoort een toetsingskader. In dit toetsingskader staat in detail beschreven wat een school geregeld moet hebben om aan bepaalde normen te voldoen. Hierbij komt ook het gewenste niveau van beveiliging aan de orde. Dit is een groot document, waarvan op dit moment niet alles voor het PO en VO even belangrijk is. Wel wordt er vanuit de Autoriteit Persoonsgevens steeds meer gekeken of scholen hun informatiebeveiliging op orde hebben en zij verwijst dan naar de ISO-maatregelen. De maatregelen vanuit het normen- en toetsingskader zullen dan ook in de volgende stappen een rol op de achtergrond spelen.*

Welke gebieden hebben te maken met IBP?

Iedere organisatie, dus ook jouw school, bestaat uit meerdere onderdelen, zoals mensen, apparatuur, programmatuur en gegevens, maar ook de organisatie zelf, de omgeving en leveranciers. IBP raakt in elke organisatie ook al deze onderdelen. Om de maatregelen te groeperen zijn er **zes clusters** gemaakt. Deze clusters komen vanuit het eerder genoemde normenkader van het MBO. Het uitwerken en toepassen van maatregelen op basis van deze zes clusters wordt zo relatief eenvoudig.

De zes clusters zijn:

1. Beleid en organisatie
2. Personeel, leerlingen en derden
3. Ruimten en apparatuur
4. Continuïteit
5. Toegangsbeveiliging
6. Controle en logging

Het is niet noodzakelijk de inhoud van de zes clusters uit je hoofd te leren; het geeft vooral inzicht en overzicht in de complexiteit. Waar nodig zullen we aangeven waar bepaalden documenten of processen betrekking op hebben. Download verderop het schema met de 6 clusters.

Wat moet je wettelijk regelen?

Vanuit het IBP-beleid zijn er een aantal onderwerpen die een school op basis van de **wetgeving** op orde moet hebben. Vanaf 25 mei 2018 wordt de huidige Wet bescherming persoonsgegevens (Wbp) vervangen door de Algemene Verordening Gegevensbescherming (AVG). Dit brengt een aantal aandachtspunten met zich mee, die we al eerder beschreven hebben bij 'Aandachtspunten AVG'. We zetten ze nog even op een rij:

- Uitgangspunten privacy (5 vuistregels2.0)
- Privacy by design / by default
- Verplichte risicoanalyse
- Documentatieplicht
- Bewustzijn creëren en voorlichten
- Gebruik digitale diensten onder de 16 jaar
- Bewerkersovereenkomsten
- Meldplicht datalekken
- Functionaris voor Gegevensbescherming
- Technische en organisatorische maatregelen

Let op: De term 'verantwoordelijke ' en 'bewerker' uit de Wbp krijgen in de AVG een andere naam! Aangezien we snel aftellen worden vanaf nu in alle documenten in de Aanpak de benamingen vanuit de Wbp vervangen door de benamingen vanuit de AVG.

- De '**verwerkingsverantwoordelijke**', is in de AVG de nieuwe naam voor de 'verantwoordelijke'.
- De '**verwerker**', is in de AVG de nieuwe naam voor de 'bewerker'.

Classificeren en risicoanalyse

IBP regel je onder andere om de continuïteit van het onderwijs en de bedrijfsvoering te waarborgen en de privacy van leerlingen en medewerkers te garanderen. Als school wil je de juiste maatregelen nemen om het risico op beveiligings- en privacy-incidenten en de eventuele gevolgen daarvan, tot een minimum te beperken.

Maar hoeveel maatregelen moet je nemen, wat is het minimum? Op welk gebied (cluster) moet je maatregelen nemen? En hoe ver moeten die maatregelen gaan? Wat zijn de grootste risico's? Allemaal vragen die je pas kan beantwoorden als je weet hoe belangrijk bepaalde gegevens en systemen zijn en als je een risicoanalyse hebt gedaan.

Dat vraagt eerst om een inventarisatie van processen en of daar persoonsgegevens in worden verwerkt.

- **Deze inventarisatie doe je gemakkelijk in de Proces-inventarisatie in Yucan.**

De AVG doet er nog een schepje bovenop. De AVG verwacht namelijk van organisaties dat zij niet alleen jaarlijks de huidige risico's in kaart brengen. Maar dat er ook bij nieuwe (ict)ontwikkelingen en gebruik van nieuwe technieken vóóraf wordt bekeken wat de mogelijke impact ervan op de bescherming van persoonsgegevens is. Dit laatste staat in de AVG beschreven als een privacy impact assessment, afgekort tot PIA of DPIA. In het Nederlands een gegevensbeschermingseffectbeoordeling. In Yucan een Proces-DPIA, want het gaat hierbij om de verwerking van persoonsgegevens in processen.

Het is dan ook van belang dat we eerst inzichtelijk krijgen hoe belangrijk bepaalde informatie en/ of informatiesystemen zijn. Dit kan door deze te **classificeren. V**ervolgens moeten we aandacht schenken aan het uitvoeren van een **risicoanalyse.**

- **Op basis van de proces inventarisatie leg je in de module kaarten in Yucan de processen en verwerkingen vast.**
- **Daarbij doe je direct de analyse en classificatie.**
- **En als een PIA nodig blijkt, dan kan je die daar ook meteen uitvoeren.**
- **En daarmee staat ook alles direct in jouw verwerkingsregister in Yucan.**
- **Moet je nog actie ondernemen om risico's te verkleinen? Vanuit de de registratie voor het bewerkingsregister EN de PIA benoem je ook eventuele verbeterpunten; de acties die je moet ondernemen om risico's te verkleinen of weg te nemen**

Door ook de classificatie vast te leggen laat je zien dat je structureel werk maakt van de beoordeling van processen en verwerkingen. Niet onbelangrijk bij de verantwoordingsverplichting die er naar de Autoriteit Persoonsgegevens onde de AVG bestaat!

Kennisnet: Alles over de PIA wordt op termijn (verwachting maart 2018) onder 'samen vooruit' in de Aanpak beschreven.

Verplichte risicoanalyse

De AVG eist van organisaties dat zij bewust omgaan met privacy. Hierbij hoort het in kaart brengen van de huidige situatie rondom IBP. Scholen moeten zich daarbij niet alleen aan de wet houden, maar ook kunnen aantonen dat zij dat doen (verantwoordingsplicht AVG).

Huidige situatie

Het is praktisch om de risicoanalyse vanuit 2 invalshoeken te benaderen

1. Voor de school als geheel. Dit is natuurlijk pas echt afgerond als alle afzonderlijke processen ook op orde zijn.
2. De afzonderlijke processen en verwerkingen

De risicoanalyse van de school als geheel

In het volgende onderdeel gaan we in op de organisatiebrede risicoanalyse; Hoe pak je dat aan en hoe gebruik je daarbij het privacy-framework van AVG-Control in Yucan.

Vanuit de analyse in het **privacy-framework** heb je beeld van de kwaliteit van het IBP van de school als geheel. Wat ontbreekt er nog? Zijn er verbeterpunten? Wat zijn daarbij de risico's voor de school als geheel?

De risicoanalyse van de afzonderlijke processen en verwerkingen

Op basis van de **proces-inventarisatie** is er zicht op de aanwezige processen en verwerkingen van persoonsgegevens. Wat zijn nu de processen met de grootste risico's? En wat zijn op dit moment de grootste risico's? Dit kunnen we in beeld krijgen door een risicoanalyse uit te voeren op de processen.

Hiermee bepaal je eerst wat de (grootste) risico's zijn.De risicoanalyse kan bijvoorbeeld antwoord geven op de vragen:

- Wat zijn de grootste risico's bij gebruik van het leerling administratiesysteem? En welke maatregelen zijn nodig om deze risico's te beperken?
- Wat zijn de risico's bij het inzetten van sociale media in de klas? Welke maatregelen moeten we nemen om dat goed te regelen?

Een risicoanalyse zal niet alleen de grootste risico's aan het licht brengen, zodat je als school weet waar je als eerste in moet investeren. Het is ook een middel om te zorgen dat iedereen hetzelfde beeld krijgt over risico's en de nadelige gevolgen voor de school. Denk bij nadelige gevolgen aan:

1. **Reputatieschade**: door incidenten die gemeld worden in de media. Bijvoorbeeld examenfraude, wachtwoorden op straat, gestolen examens. Dit is slecht voor het imago van een school.

2. **Financiële schade**: als leerlinggegevens niet juist zijn kan de bekostiging van deze leerlingen in gevaar komen; je niet houden aan de privacywetgeving kan financiële consequenties hebben, zoals het niet melden van een datalek.

3. **Continuïteit** het onderwijs: Cybercrime en DDos-aanvallen kunnen het onderwijs enorm verstoren.

4. **Wet en regelgeving**: er moet aantoonbaar voldaan worden aan de AVG.

5. Risico's in de **cloud**: toepassingen in de cloud leveren specifieke aandachtspunten op zoals eigenaarschap, toegang, privacy en continuïteit van de dienstverlening van externe partijen.

6. Te beperkt **kennisniveau**: ontwikkelingen gaan snel, de eisen om te voldoen aan wet- en regelgeving worden strenger en de risico's groter. Onvoldoende kennis kan tot gevolg hebben dat er onjuiste beslissingen worden genomen ten aanzien van informatiebeveiliging en privacy met alle gevolgen van dien.

Een risicoanalyse lijkt een moeilijke bezigheid, maar met behulp van het privacy-framework en de proces-DPIA's in Yucan heb je dit als school goed op de rit. Op sommige gebieden heb je misschien een expert nodig. Denk daarbij aan Ict, organisatieadviseur, privacy-specialist of een jurist om bepaalde aspecten meer diepgaand te beoordelen.

Het uitvoeren van een proces-inventarisatie, classificatie en proces-DPIA's noemden we al:

- **Op basis van de procesinventarisatie leg je in de module kaarten in Yucan de processen en verwerkingen vast.**
- **Daarbij doe je direct de analyse en classificatie.**
- **En als een PIA nodig blijkt, dan kan je die daar ook meteen uitvoeren.**
- **Daarmee staat ook alles direct in jouw verwerkingsregister in Yucan.**

Daarna kijk je welke maatregelen nodig zijn om die risico's tot een minimum te beperken. Deze maatregelen kun je vervolgens samen met de wettelijke verplichtingen inplannen voor de komende tijd.

- **Moet je nog actie ondernemen om risico's te verkleinen? Vanuit de PIA start je eenvoudig een verbeterplan.**
- **Zo geef je ook direct vorm aan de aanpak die in de AVG verplicht gebaseerd is op de PDCA.**

Hoe doe je dit?

- **Onder projecten start je een verbeterplan en koppelt deze aan één of meer registraties (en PIA's) om de maatregelen uit te werken en te plannen (deadlines en staussen blijven zichtbaar).**
- **Je kunt het verbeterproject hier ook aan iemand geven om uit te werken en op te pakken.**

Risicoanalyse - uitvoering

Het doel van de jaarlijkse risicoanalyse is het school-breed bepalen wat de grootste risico's zijn op het gebied van informatiebeveiliging en privacy. Het is belangrijk dat de uitkomst van de risicoanalyse weergeeft hoe de hele school erover denkt.

Verzamel de juiste mensen

Een risicoanalyse in de vorm van een workshop werkt prettig. Het is belangrijk dat je mensen met verschillende rollen en taken hierbij betrekt. Denk daarbij aan de bestuurder, een docent, een ict-coördinator, iemand van P&O en de administratie en misschien zelfs een stagiair. Al die mensen hebben verschillende inzichten en belangen. Wat een groot risico is voor de administratie, is misschien een klein risico voor de docent. Maak de groep niet groter dan drie tot zes personen.

Voorbereiden via het AVG Privacy-Framework

Nodig de groep uit om als voorbereiding het **privacy-framework** in Yucan te doorlopen (team-aanpak in Yucan). Alle voor de school belangrijke aandachtsgebieden komen langs.En laten direct ook zien waar u voor de wet (AVG) aan moet voldoen.

Vraag ze op de afzonderlijke onderwerpen (waarvan ze vinden of weten dat ze er een mening en bijdrage over kunnen hebben) aan te geven hoe de school er bijstaat. En vraag ze om daarbij een toelichting te geven en verbeterpunten te benoemen!

- **De input van de groep gebruik je voor de brainstorm en discussie**
- **Bij alle verbeterpunten kan je in Yucan via de behandellijst compacte risico-analyses doen. En er een prioriteit aan meegeven.**
- **Zo bepaal je bij een brainstorm en discussie gezamenlijk waar de risico's zitten en wat als eerste wordt opgepakt.**

Hulpmiddelen

Zorg voor flipovervellen, post-its en pennen om uitkomsten vast te leggen. Zorg voor een internetaansluiting en een beamer.

Spreek af hoe je een risico opschrijft.

Het moet in ieder geval een begrijpelijke omschrijving zijn, met een inschatting van de kans, en van de impact. Ook over de kans en de impact maak je afspraken. Wat is klein en wat is groot? (zie onderstaande voorbeeld) Op die manier kun je de latere discussie veel makkelijker voeren.

Een risico is een <gebeurtenis>, die leidt tot <een gevolg> door een bepaalde <oorzaak>.
Een risico wordt aangegeven door kans x impact

Kans: kans op optreden van een risico

1: Klein	kan minder dan jaarlijks voorkomen
2: Middel	kan meerdere keren per jaar voorkomen
3: Groot	kan dagelijks voorkomen

Impact: de gevolgen als een risico optreedt

1: Klein	verstoring niet-primair proces, alleen intern merkbaar
2: Middel	verstoring primair proces, extern merkbaar, snel opgelost
3: Groot	verstoring primair proces, reputatieschade, langdurig

Een risico wordt aangegeven door kans x impact

Brainstormen en discussie

De risico beoordeling kan je direct in Yucan doen maar er ook voor kiezen dit anders aan te pakken. Wat goed werkt is het volgende:

Login op Yucan en open uw werkruimte in de conclusiestap om de antwoorden van de groep te bekijken en te bespreken.

Neem de eerder genoemde aandachtsgebieden uit het framework en de output van de groep bij de bijbehorende onderwerpen als uitgangspunt.

Neem een uur de tijd om zoveel mogelijk risico's op te schrijven. Kijk nog eens naar de presentatie. Plak deze per aandachtsgebied op een flipover. Noteer de resultaten en sorteer ze. Zoek de discussie op over welk (grootste) risico bovenaan komt te staan. Plaats het vervolgens in de behandellijst van Yucan om ook op termijn grip te houden.

Bepaal de maatregelen

De laatste stap is het bepalen van de maatregelen. Doe dat in de groep door bijvoorbeeld weer te werken met post-its. Of noteer ze direct bij het verbeterpunt in de behandellijst in Yucan. Daarbij geef je aan waarmee je aan de slag gaat. **En daarvoor start je in Yucan bijvoorbeeld een verbeterproject (zie ook verderop onder 'plan acties in + a, b en c)**.

Behulpzaam omdat het je handvatten geeft om verbetering doelmatig aan te pakken **EN** het direct te koppelen aan de verbeterpunten die je had gevonden. Zo blijft de samenhang in tact en kan je ook in de loop van de tijd bijhouden hoe voortgang is en of verbeterpunten worden opgelost.

Klaar?

Bijna! Het is nuttig om de resultaten samen te vatten in een memo voor de bestuurder. Meestal wordt gevraagd om de hoofdlijnen waarin naar voren komt:

- De aanpak
- De grootste risico's
- De meest belangrijke maatregelen

Gebruik hiervoor de **rapportagemogelijkheden in Yucan**. Die bieden je met een druk op de knop:

- Overzicht van de stand van zaken (evaluatierapport)
- Overzicht van de verbeterpunten, risico's en prioriteitstelling en beoogde maatregelen

(behandellijst met prioriteiten)

(op ieder moment met een druk op de knop beschikbaar als pdf of om op te slaan in Yucan)

De bestuurder of directeur heeft dan inzicht in de uitkomst van de risicoanalyse en de onderbouwing van de te nemen maatregelen. Na een akkoord kunnen vervolgens de voorgestelde maatregelen de komende tijd opgepakt worden.

Plan acties in

Tot nu toe is gekeken naar de onderwerpen die vanuit de AVG extra aandacht vragen. Ook zijn uit de risicoanalyse de nodige maatregelen voor jouw organisatie naar voren gekomen. De verbeterplannen zijn er. Maar alles in één keer realiseren in niet mogelijk, maak daarom een actieplan. Hierin geef je aan welke acties je eerst gaat uitvoeren en wat je later oppakt.

Maak gebruik van je bestaande jaarkalender om te bekijken wat wanneer gedaan kan worden. Wat is haalbaar? En wie moeten er een rol nemen?

- **Bekijk de behandellijst en de verbeterplannen die zijn aangemaakt.**

Het IBP-beleid en de onderliggende documenten en procedures moeten eigenlijk regelmatig, liefst elk jaar, weer eens bekeken worden om er zeker van te zijn dat alles nog actueel is. Plan deze jaarlijkse activiteit gelijk in.

Nu de grootste risico's bekend zijn en de maatregelen gekozen zijn kunnen de bijbehorende acties uitgewerkt worden en ingepland. Hou bij het plannen van acties goed rekening met de eisen vanuit de AVG. De AVG legt immers een aantal wettelijke verplichtingen op, waarbij je als instelling moet kunnen aantonen dat hieraan wordt voldaan.

Hoe helpt de Aanpak?

In deze Aanpak is vast gekeken naar wat er **wettelijk** vanuit de AVG geregeld moet worden als het gaat om IBP. Op basis daarvan is de module 'Realiseren' als volgt opgebouwd:

1. **'*Realiseren - Aan de slag*':** Bevat met name de onderwerpen, die zich afspelen binnen de muren van de school.
2. **'*Realiseren - Goed op weg*':** Laat zien wat je moet regelen als je te maken krijgt met de wereld buiten je school. Zoals afspraken rondom sociale media, uitwisseling van leerlinggegevens/-dossiers et cetera
3. **'*Realiseren - Samen vooruit*':** Richt zich op grotere onderwerpen, die elke organisatie vanuit de AVG geregeld moet hebben. Dit zijn onderwerpen die we samen op kunnen pakken. Zoals het aanstellen van een Functionaris voor gegevensbescherming, de (DPIA), het voldoen aan de documentatieplicht en daarmee het ontwikkelen van een dataregister, het omgaan met (D)DOS en het continue verbeteren.

Aan de hand van deze planning en alles wat je hebt vastgelegd en nog gaat vastleggen in Yucan kun je aantonen dat alle elementen de aandacht hebben en dat je stapsgewijs IBP op orde gaat krijgen. Het laat zien dat er aan gewerkt wordt om (aantoonbaar) te voldoen aan de AVG. Je kunt het op ieder moment aantonenen maar hebt vooral ook zelf altijd zicht op hoe het er voor staat.

2.a. Aan de slag

In de eerste module van realiseren richten we ons als eerste op wat je al geregeld had moeten hebben sinds het invoeren van de Wet bescherming persoonsgegevens in 2001. Het gaat om onderwerpen, die *gisteren* al klaar hadden moeten zijn. Maar ook om onderwerpen, waarvoor we binnen de muren

van de school, achter de voordeur, afspraken moeten maken.

Aan bod komen onder andere:

- Procedure melden **beveiligingsincidenten** / meldplicht **datalekken**
- **R**echten van betrokkenen vastleggen
- **Privacyreglement** voor leerlingen en medewerkers
- **Afspraken met leveranciers** maken over het gebruik van leerlinggegevens en het afsluiten van **verwerkersovereenkomsten**
- Het **gebruik** van **beeldmateriaal**

In deze aanpak is al rekening gehouden met de invoering van de Europese Algemene Verordening Gegevensbescherming (25 mei 2018). Verder wordt uitgegaan van de meest recente tekst van de Wet bescherming persoonsgegevens. Hierdoor voldoet deze aanpak IBP zowel aan de huidige als toekomstige privacywetgeving!

Ok, aan de slag!

Procedure melden beveiligingsincidenten

Op 1 januari 2016 is de meldplicht datalekken ingegaan. Deze meldplicht houdt in dat alle organisaties (dus ook onderwijsorganisaties) een datalek moeten melden bij de Autoriteit Persoonsgegevens. In een aantal gevallen moet het datalek ook gemeld worden bij de betrokkenen (de personen van wie de persoonsgegevens zijn gelekt).

Verschil datalek en beveiligingsincident

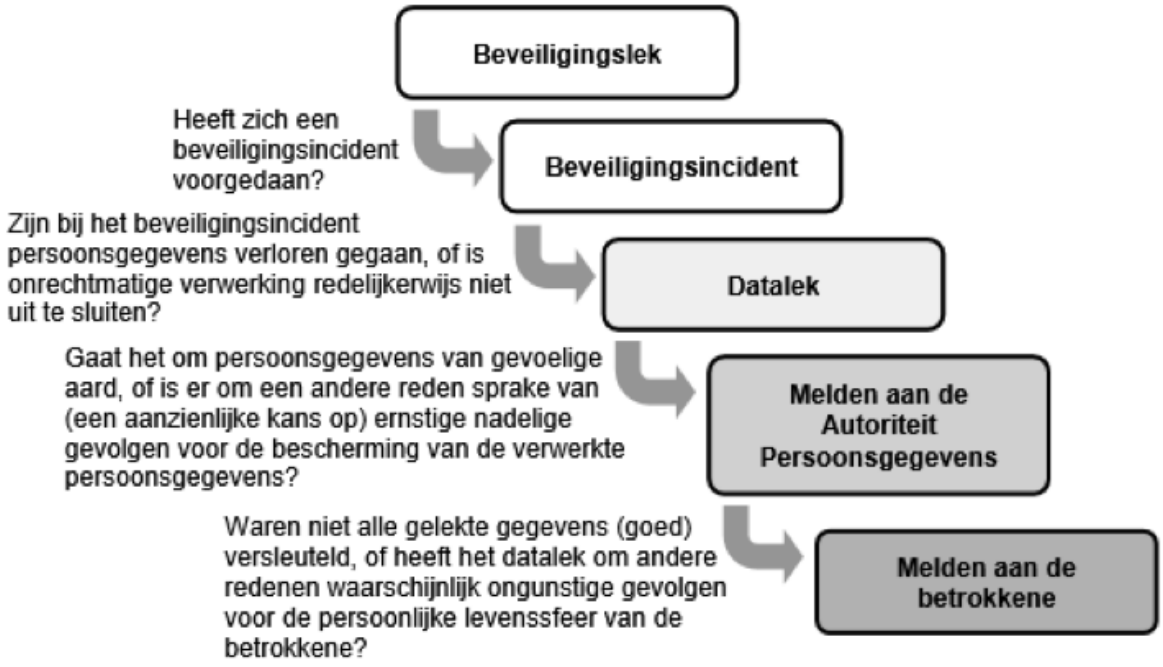
- Een **beveiligingsincident** is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.
- Een **datalek** is een beveiligingsincident, waarbij persoonsgegevens verloren raken of onrechtmatig worden verwerkt (opgeslagen, aangepast, verzonden enz.).

Alle datalekken zijn dus beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken!

LET OP: Zorg ervoor dat alle medewerkers weten wat een beveiligingsincident of een datalek is, en waar ze een beveiligingsincident moeten melden. Medewerkers moeten weten dat zij niet alleen het verlies van een USB stick, een gestolen laptop et cetera met daarop persoonsgegevens van leerlingen en/of medewerkers moeten melden. Maar ook melding moeten doen van die verstuurde e-mail naar de verkeerde geadresseerde.

Wel of niet melden

Het is belangrijk dat je weet wanneer je een gebeurtenis moet melden bij de Autoriteit Persoonsgegevens (AP) en eventueel ook aan de betrokkene. De AP heeft een richtsnoer meldplicht datalekken gepubliceerd (zie download verderop), waarin het onderstaande schema staat. Dit schema helpt om de juiste afwegingen te maken en is verderop te downloaden om in het procotol op te nemen.



Protocol en incidentenregistratie

Naast de meldplicht is er ook de verplichting om alle **beveiligingsincidenten registreren.** Dat geldt óók voor alle incidenten die niet gemeld hoeven te worden. De Autoriteit Persoonsgegevens kan altijd om inzage hiervan vragen.

- **Datalekken registreer je eenvoudig in Yucan onder kaarten, zo heb je direct ook je register voor datalekken op de rit.**
- **Je ziet daar ook direct wat je wanneer in welke situatie moet vastleggen EN moet doen om aan de AVG te voldoen.**

Om alles rondom het melden van datalekken en het registreren goed te regelen is belangrijk om een protocol beveiligingsincidenten en datalekken op te stellen. Een voorbeeld staat onderaan deze pagina. Dit template kun je aanpassen aan de situatie op jouw school. Zorg er wel voor dat de onderstaande punten in het protocol worden meegenomen.

- Zorg dat het voor iedereen duidelijk is een incident gemeld moet worden. Stel bijvoorbeeld het e-mailadres van de manager-IBP / security-officer / informatie-manager beschikbaar.
- Een technisch onderzoek kan zowel intern als extern belegd zijn. Dit laatste zal het geval zijn als een school het IT-beheer heeft uitbesteed. Benoem dit in het protocol.
- De manier van communiceren met betrokkenen en eventueel met de pers. Leg dit vast in het protocol.
- Het omgaan met signalen van buitenaf over een mogelijk datalek.
- Onder welke omstandigheden je gebruik wilt/moet maken van externe deskundigen.
- Registreer en archiveer alle incidenten. Als je niet de beschikking hebt over een passend registratiesysteem (of dit in Yucan wilt doen), dan kun je gebruik maken van het document onder aan deze pagina om incidenten te registreren.
- Maak het melden van een incident door de ontdekker makkelijk door een standaard meldingsformulier te maken. Het onderstaande document ‘Incidenten registratie’ bevat een tabblad '*Meldingsformulier ontdekker*'. Hierin staan de basis gegevens waarmee een dergelijk formulier gemaakt kan worden.

Rechten van betrokkenen

Door de Algemene Verordening Gegevensbescherming (AVG) krijgen betrokkenen (degenen van wie persoonsgegevens worden verwerkt) meer mogelijkheden om voor zichzelf op te komen als het gaat om de verwerking van hun gegevens. Onder de AVG zijn de rechten van betrokkenen verder uitgebreid.

Rechten

Als het gaat om de rechten van betrokkenen is transparantie een belangrijke voorwaarde. Leerlingen en ouders moeten actief betrokken worden en verteld worden wat hun rechten zijn. De organisatie moet betrokkenen de gelegenheid geven hun rechten eenvoudig en met redelijke tussenpozen uit te kunnen oefenen. Zorg ervoor dat zowel leerlingen als ouders en ook medewerkers goed geïnformeerd zijn over hun rechten en de procedure om van hun rechten gebruik te kunnen maken.

Maar welke rechten hebben leerlingen en/of hun ouders (als de leerlingen jonger zijn dan 16 jaar) en medewerkers eigenlijk? In het document 'transparantie en rechten betrokkenen' wordt dit verder uitgewerkt.

Procedure

Informeer ouders en leerlingen op het moment dat zij – voor het eerst – persoonsgegevens actief en bewust gaan delen met de school over hun rechten. Vertel en leg uit welke gegevens er worden vastgelegd of doorgegeven aan een andere instantie en waarom. Zorg ervoor dat betrokkenen weten hoe zij van hun rechten gebruik kunnen maken. Leg in een procedure vast hoe betrokkenen hun rechten kunnen uitoefenen. Neem rechten betrokkenen op in het leerlingstatuut en/of in het privacyreglement. Zet ook op de website en eventueel in de schoolgids meer achtergrondinformatie over privacy en de rechten van betrokkenen.

In onderstaand document zijn de afspraken en procedures rondom de rechten van betrokkenen op een rij gezet.

Let op

- **Rechten van betrokkenen en procedures worden ook behandeld in het privacy-framework (hoofdstuk 7).**
- **Je hebt daar een duidelijk overzicht van wat daarbij moet gebeuren en direct ook een checklist tot je beschikking.**

- **Het beschrijven van procedures doe je eenvoudig in de module 'kaarten' in Yucan.**
- **Deze kan je ook aan de onderwerpen in het privacy framwork koppelen. Zo heb en houdt je altijd overzicht.**

Privacyreglement

Iedere school verwerkt persoonsgegevens van personeel en leerlingen. In het privacyreglement leg je vast voor welke doelen je persoonsgegevens registreert. Het gaat hierbij niet alleen om gewone persoonsgegevens zoals naam, geboortedatum en overige contactgegevens, maar soms ook om bijzondere persoonsgegevens met betrekking tot bijvoorbeeld gezondheid, afkomst en godsdienst.

In het privacyreglement zijn in ieder geval alle onderdelen en processtappen beschreven die je in het vorige onderdeel hebt geregeld. Het bevoegd gezag is verantwoordelijk voor de bescherming van de privacy van leerlingen en medewerkers en stelt dan ook het privacyreglement vast. Het privacyreglement is daarmee voor alle scholen die onder hetzelfde gezag vallen van toepassing.

- **In de module kaarten vind je een handig format voor het opstellen van een privacyreglement.**
- **Je hebt daar direct in beeld wat er in aan de orde moet komen.**
- **Als je dit daar vastlegt heb je het altijd binnen je AVG dossier beschikbaar.**

Via onderstaande stappen stel je het privacyreglement voor jouw school op.

Stap 1. Ken de wetgeving

Voor je met het privacyreglement aan de gang gaat is het goed om te weten wat er in de wet staat. Alle wetgeving vind je via de inhoudsopgaaf onderin. De vragen en praktische toelichting van de AP - die je ook vindt in de inhoudsopgaaf - geeft je hierover handige beschrijvingen.

Stap 2. Stel een privacyreglement op

Kennisnet helpt scholen om hun privacyreglement op te stellen door een voorbeeld-reglement ter beschikking te stellen. Deze kun je hieronder downloaden en voor je eigen school aanpassen of in Yucan aanmaken (zie boven).

***Let op**: het privacyreglement gaat over de rechten en plichten van betrokkenen. Dat betekent dat de (G)MR het reglement moet goedkeuren.*

Stap 3. Communiceer over privacy

Richting vaste medewerkers worden de afspraken rondom de bescherming van persoonsgegevens vaak als onderdeel van de arbeidsovereenkomst vastgelegd. Voor minder vaste medewerkers, stagiaires en ingehuurd personeel worden deze afspraken vaak niet opgenomen in de contracten. In dat geval kun je gebruik maken van een geheimhoudingsverklaring. Zie onderstaande download. Deze staat ook in de bibliotheek van jouw werkomgeving en heb je zo beschikbaar in jouw AVG dossier.

Een school heeft een informatieplicht en moet uitleggen hoe de school met de gegevens van leerlingen omgaat. Ouders hebben daarover recht op volledige transparantie van de school. Onderstaand kun je praktische voorbeeldteksten downloaden die scholen kunnen gebruiken om ouders te informeren over privacy op school. Bijvoorbeeld door ze op te nemen in de schoolgids of op de website. Deze staat ook in de bibliotheek van jouw werkomgeving en heb je zo beschikbaar in jouw AVG dossier.

Wachtwoord beleid

Veel applicaties die in het PO en VO gebruikt worden zijn online. Leerlingen moeten allemaal inloggen met een gebruikersnaam en een wachtwoord. Hoe ga je daar als school nu mee om en hoe hou je dat praktisch uitvoerbaar?

Hoe moet het niet?

Kies als school niet voor één simpel wachtwoord voor elke leerling om veel 'gedoe' te voorkomen.

De zorg zit niet zo zeer in het feit dat leerlingen onderling bij elkaar kunnen kijken, maar meer in de onveiligheid en risico's naar buiten toe. Uit de programma's kunnen veel gegevens afgeleid worden, totaal scores, gesprekken via de chat enz.

Als het gaat om digitale vaardigheden en IBP, dan spreekt het vanzelf dat je leerlingen zo vroeg mogelijk leert om zorgvuldig om te gaan met hun persoonsgegevens en dus ook met hun wachtwoorden. Dit sluit aan bij het mediawijs maken van leerlingen en de *ICT-basisvaardigheden.* En dat leer je ze niet door ze allemaal hetzelfde wachtwoord te geven…

Hoe ga je dat nu aanpakken?

De drie basisregels voor wachtwoorden zijn voor iedereen gelijk. Ook jonge kinderen moeten we deze aanleren:

1. **Je wachtwoord mag je nooit delen, dat is iets van jou.**
2. **Je wachtwoord mag niet makkelijk te raden zijn (bijvoorbeeld een 'wachtzin'** Mijnkatisliefennietgroen!**)**
3. **Je wachtwoord mag je niet hergebruiken. Gebruik voor alles een eigen wachtwoord.**

De *eerste regel* sluit dus uit dat wachtwoorden voor alle kinderen hetzelfde zijn. Een wachtwoord is persoonlijk.

De *tweede regel* heeft te maken met complexiteit. Hier wordt het wat lastiger, want kinderen moeten het wel kunnen onthouden. Mensen mogen je wachtwoord niet kunnen raden, maar ook computers niet.

- Mensen kunnen je wachtwoord makkelijk raden wanneer je iets heel simpels of bekends gebruikt, zoals de naam van je hond.
- Computers kunnen je wachtwoord makkelijk raden wanneer het kort is.

Vroeger werden korte, maar complexe wachtwoorden aanbevolen. Deze zijn voor een mens moeilijk te raden (maar wel te onthouden). Echter de huidige snellere computers kunnen deze wachtwoorden wél snel achterhalen. Een lang wachtwoord of een 'wachtzin' is dan ook beter dan een kort complex wachtwoord.

De *derde regel* zal voor jonge kinderen (PO) niet realistisch zijn. In het VO kun je deze regel wel hanteren.

Voorbeeld

Een pragmatische en effectieve oplossing kan zijn om (jonge) kinderen een zinnetje te laten maken. Ga hiervoor met de leerling als volgt te werk:

1. Maak een goed te onthouden zin, zoals 'Mijn kat is lief en niet groen'

2. Verwerk ook een hoofdletter, cijfer en / of leesteken in het wachtwoord, bijvoorbeeld Mijnkatisliefennietgroen!

Responsible disclosure

Voor schoolbesturen speelt ict een steeds grotere rol in de ondersteuning van het onderwijs. Het is hun verantwoordelijkheid te zorgen dat het onderwijs altijd door kan gaan en dat de veiligheid van een informatiesysteem en (software)producten wordt gegarandeerd.

Ondanks alle aandacht voor de beveiliging van systemen kan het voorkomen dat er toch een zwakke plek, een kwetsbaarheid, is. Als iemand een zwakke plek in één van de systemen heeft gevonden hoor je dat als school graag zo snel mogelijk, zodat de juiste maatregelen kunnen worden getroffen.

Ook al worden kwetsbaarheden zonder kwade bedoelingen bij toeval ontdekt, vaak worden ze niet gemeld bij de scholen. Wanneer scholen nadenken over hoe ze omgaan met beveiligingsproblemen en dit duidelijk naar buiten communiceren weten medewerkers en leerlingen beter waar ze aan toe zijn wanneer ze een kwetsbaarheid willen melden. Dit voorkomt onzekerheid en paniek aan beide kanten en beperkt eventuele schade zoveel mogelijk.

Het responsible disclosure beleid heeft als doel om de drempel tot het melden van deze kwetsbaarheden te verlagen, waardoor het beveiligingsniveau van informatiesystemen en het netwerk verhoogt kan worden en schade voor de schoolbestuurder kan worden beperkt en/of voorkomen. Het responsible disclosure beleid is een oplossing om op een maatschappelijk verantwoorde en effectieve manier om te gaan met het melden van ict-kwetsbaarheden. Het geeft de mogelijkheid om af te spreken dat bij eventueel strafrechtelijk handelen van de melder geen aangifte zal worden gedaan of civielrechtelijke stappen zullen worden ondernomen.

Voor zowel de school als voor de melder schept het beleid duidelijkheid in de verantwoordelijkheden die beide partijen hebben. Het aanbieden van een beloning kan leerlingen mogelijk (extra) motiveren om een kwetsbaarheid te melden.

Afspraken met leveranciers: verwerkersovereenkomsten

In het IBP-beleid is al aangegeven dat een school verantwoordelijk is voor de zorgvuldige omgang met de persoonsgegevens van leerlingen. Om dit te kunnen garanderen zijn goede afspraken met aanbieders van digitale leermiddelen van belang.

Let op: In de Aanpak gebruiken we vast de benamingen vanuit de AVG, dus we hebben het over **ver**werkers, **ver**werkersovereenkomsten en **verwerkingsverantwoordelijke**.

Model verwerkersovereenkomst

Dankzij het convenant '**Digitale Onderwijsmiddelen en Privacy 2.0** is het voor scholen eenvoudiger om afspraken te maken met leveranciers. Belangrijkste punt in het convenant is de rolverdeling: scholen hebben de regie op wat er gebeurt met de persoonsgegevens. Dit mag je niet overlaten aan een leverancier (een verwerker). De school beslist wat de leverancier wél en niet met de gegevens mag doen.

Voor een groot deel is het convenant een vertaling van eisen uit privacywetgeving naar de onderwijspraktijk. Het convenant gaat niet alleen over het gebruik van digitaal leermateriaal, maar ook over school- en leerling administratiesystemen zoals ParnasSys, Magister en SOM.

Bijlagen bij het model

Bij het convenant hoort een model verwerkersovereenkomst waarmee je schoolbestuur (de verwerkingsverantwoordelijke) de juiste afspraken maakt met leveranciers. Er is afgesproken met vertegenwoordigers van de leveranciers, dat de tekst van het model zo belangrijk is, dat het niet de bedoeling is om het model te wijzigen. Als dat echt noodzakelijk is, moet de leverancier dat in een *aparte* bijlage uitleggen.

Bij de model verwerkersovereenkomst horen 2 bijlagen. In de **privacybijsluiter** wordt uitgelegd wat het product van de leverancier doet, welke gegevens er worden uitgewisseld met de leverancier, wat het doel is van die uitwisseling en of de leverancier andere bedrijven inschakelt (dit noemen we subbewerkers). De tweede bijlage is de beschrijving van de **technische en organisatorische beveiligingsmaatregelen** die zijn genomen. Daarin staat bijvoorbeeld wat de afspraken zijn in geval van een beveiligingsincident zoals een datalek.

Verderop kun je de 'Model Bewerkersovereenkomst Versie 2.0' downloaden, die je als template kunt gebruiken om afspraken met leveranciers vast te leggen.

A**andachtspunten gebruik digitale onderwijsmiddelen**

De onderstaande checklist gebruik digitale onderwijsmiddelen laat in een aantal stappen zien waar je rekening mee moet houden bij het inzetten van digitaal lesmateriaal en wat je eventueel moet regelen met de leveranciers ervan.

- Checklist gebruik digitale onderwijsmiddelen (inclusief een schematische beslisboom) (donload zie onder)

Als een leverancier het convenant niet heeft ondertekend is het extra belangrijk om de privacy afspraken goed vast te leggen. De 'checklist afspraken leveranciers' bevat de onderwerpen die De Autoriteit Persoonsgegevens benoemt om in een schriftelijke overeenkomst tussen verwerkingsverantwoordelijke en verwerker vast te leggen (download zie onder).

Certificeringsschema; een veilige en betrouwbare onderwijsketen

Het is voor onderwijsinstellingen lastig om eenvoudig vast te stellen of een leverancier de juiste beveiligingsmaatregelen heeft genomen. Omgekeerd is het voor leveranciers niet eenvoudig om aan te tonen dat zij tenminste aan de minimale eisen voldoen. Het hanteren van een eenduidige meetlat lost dit probleem op.

Digitale leermiddelen en (administratie)systemen moeten soepel werken en in navolging van de AVG moeten de gegevens, die hierbij verwerkt worden, betrouwbaar en goed beveiligd zijn.
Het **certificeringsschema voor informatiebeveiliging** is die meetlat, het is de standaard die hiervoor is ontwikkeld.

Dit certificeringsschema is enerzijds bedoeld voor leveranciers van ict-toepassingen in de onderwijsketen. Zij kunnen op een eenduidige manier aantoonbaar maken dat ze de informatiebeveiliging en privacy van hun diensten en producten op orde hebben.

Anderzijds is het certificeringsschema bedoeld voor onderwijsinstellingen. Bij het specificeren van informatiebeveiligingseisen kun je eenvoudig verwijzen naar het certificeringsschema, in plaats van specifieke eisen te stellen met betrekking tot (veelal technische) maatregelen. Je kan als school met het toetsingskader eenvoudiger (laten) toetsen of de leverancier hun informatiebeveiliging op orde heeft. Vraag aan de leverancier of zij hun dienst hebben beoordeeld met het certificeringsschema en of ze een rapportage kunnen overleggen. Hoe meer scholen dit vragen van hun leveranciers, hoe meer leveranciers het ook als standaard zullen gaan zien. Op deze manier kunnen we samen de beveiliging in de hele keten naar een hoger niveau brengen. Kijk voor meer informatie over het certificeringsschema bij Edu-K

Gebruik beeldmateriaal leerlingen

Schoolfeestje, gezellig! En nu die filmpjes en foto’s gelijk op de website... Nee dus. Foto's en video's van leerlingen zijn persoonsgegevens, daarom gelden er vanuit de privacy wetgeving eisen voor het gebruik van beeldmateriaal.

Toestemming vragen

Het gebruiken van beeldmateriaal, het delen van foto's en video's van leerlingen door scholen, vormt zelden een probleem en is meestal goedbedoeld. Toch eist de wetgever dat de school vooraf toestemming vraagt aan ouders voor het gebruik van beeldmateriaal van leerlingen als de leerling jonger is dan 16 jaar. Als de leerling 16 jaar of ouder is moet hij/zij zelf toestemming geven. Zonder die toestemming mag je geen foto’s en video’s van leerlingen gebruiken.

Bij het vragen van toestemming zijn drie punten van belang:

- De toestemming moet **in vrijheid** gegeven worden; toestemming moet geweigerd kunnen worden zonder dat leerlingen daardoor benadeeld zouden worden.
- De toestemming moet **'ondubbelzinnig'** zijn. Toestemming mag niet verborgen zijn in schoolregels en er mag niet van uitgegaan worden dat ouders toestemming geven als zij niet reageren. Ouders/verzorgers moeten **expliciet** kunnen aangeven waar ze wel of geen toestemming voor verlenen. De school moet de toestemming altijd kunnen aantonen.
- De toestemming moet **specifiek** zijn. Het moet duidelijk zijn waar toestemming voor gegeven wordt en met welk doel. Zorg voor **gelaagde** toestemming: wil je toestemming voor foto’s op de website, in de schoolgids, nieuwsbrief of in sociale media? De keuze moet duidelijk aan te geven zijn, bijvoorbeeld door een kruisje in een vakje te zetten bij bepaalde type media (foto's/film) of bij bepaalde uitingen (website, schoolkrant, etc.).

Zorg dat je als school vóóraf de juiste afspraken hebt gemaakt en dat iedereen ook weet wat die afspraken zijn. Lees voor extra informatie ook het artikel Nieuwe beleidsregels voor gebruik beeldmateriaal leerlingen.

Onderstaande voorbeeld brief (download) kan gebruikt worden om toestemming te regelen.

Tip: Foto's veilig delen

Naast toestemming vragen is de school ook verantwoordelijk voor het **veilig delen** van beeldmateriaal. Een openbaar fotoalbum mag niet meer. Plaats daarom foto's op een beveiligde site waarbij ouders moeten inloggen. Hou er wel rekening mee dat ook hier alléén foto's komen van kinderen waarvan de ouders toestemming hebben gegeven om foto's te delen!

Filmen/fotograferen door ouders

Het aantal ouders dat met camera's en smartphones foto's maakt of filmt op school is in de afgelopen jaren flink toegenomen. Ook deze foto’s komen al snel op Facebook of YouTube. En wat als een ouder de foto van de beveiligde site kopieert en zelf deelt?

Ook hier geldt dat een school voor álle kinderen een veilige omgeving moet zijn, en niet een plek waar zij (en hun ouders) het risico lopen ongewenst gefotografeerd te worden. Maar het maken van foto’s en video’s door ouders op school kun je moeilijk verbieden. En als een ouder de foto kopieert en zelf deelt neemt de ouder daar de verantwoordelijkheid voor: de school kan niet verbieden dat ouders die foto's overnemen en verder delen (zelfs niet als dat bijvoorbeeld publiek op Facebook is)... Je kan er wel **afspraken** over maken, want een school is niet zomaar een openbare plaats waar iedereen toegang toe krijgt.

De volgende artikelen geven aanvullende informatie. Lees ze goed door, zodat je de do's en don'ts op jouw school met alle betrokkenen kunt delen.

- **Foto's van leerlingen gebruiken? Zo mag het wel!**
- **Mogen leraren en ouders foto’s maken van leerlingen?**
- **Leidraad omgaan met online verspreiding ongewenste beelden**

Informatieplicht

Het realiseren van het IBP-beleid zal voor een groot deel uit **informeren** bestaan. De Algemene Verordening Gegevensbescherming (AVG) legt vanaf 25 mei 2018 een wettelijke verplichting op met betrekking tot informatieverstrekking. Schoolbesturen moeten de betrokkenen nog meer informeren over hoe zij met hun persoonsgegevens omgaan.

Een schoolbestuur moet transparant zijn over de privacyafspraken en -processen, en daar proactief informatie over verstrekken. Dat betekent bijvoorbeeld dat er in de schoolgids of op de website voldoende informatie is te vinden over hoe de school omgaat met persoonsgegevens, welke afspraken er zijn rondom privacy en welke maatregelen er zijn getroffen om de persoonsgegevens te beschermen.

Eigenlijk moet er bij iedere stap die je zet, elk proces dat je inregelt en ieder document dat je vastlegt een lampje gaan branden met de vraag:

Wie moet ik hierover inlichten en op welke manier?

- Medewerkers
- Leerlingen
- Ouders

Communiceer!

Het met regelmaat praten over het belang van informatiebeveiliging en privacy helpt om het bewustzijn bij iedereen te vergroten. In het hoofdstuk 'Communiceren' bieden we je tips hoe je met zowel medewerkers, leerlingen als ouders over deze onderwerpen een dialoog kunt starten. Wil je al direct van start, dan kun je via onderstaande links meteen het gewenste onderwerp opzoeken:

2.b. Goed op weg

Dat gaat lekker! In de vorige module heb je gerealiseerd wat je *gisteren* al geregeld moest hebben binnen de deuren van de eigen organisatie. In deze module kijken we naar de onderwerpen die naar voren komen als de voordeur opengaat, als we gebruik gaan maken van sociale media of gegevens moeten uitwisselen.

In deze module gaan we aan de slag met:

- **Afspraken over sociale media**
- **Gedragscode ict en internetgebruik**
- **Uitwisselen van gegevens**
- **Toegang tot gegevens**

Deze onderwerpen kun je in iedere gewenste volgorde oppakken. Misschien heb je bepaalde zaken al prima op orde; zelfs dan raden we je aan om toch even het betreffende onderwerp door te lezen, wellicht dat je nog verbeterpunten tegenkomt.

Zet ook deze activiteiten op de jaarkalender, zodat je het niet vergeet. Als er gevraagd wordt hoe het er voor staat, dan kan je laten zien wanneer je het opgepakt wordt .

Succes!

Afspraken over sociale media

Deel je artikelen met collega's via Twitter? Heeft jouw school een Facebook-pagina? Posten jullie video's van musicals op YouTube? Heb je al een Snapchat-account? En hoe up-to-date is je LinkedIn-profiel... Vrijwel iedereen gebruikt tegenwoordig wel een of meerdere 'social media'. Media waarop wij als gebruikers *zelf* berichten kunnen zetten, in tekst, video, audio of afbeeldingen. Vaak erg handig en leuk, maar uiteraard ook met de nodige risico's.

Iedere school heeft wel positieve en negatieve verhalen te vertellen over het gebruik van social media door leerlingen (en medewerkers!). Om de online veiligheid van iedereen op school te verbeteren stellen scholen protocollen op, organiseren ze informatieavonden of sluiten ze bijvoorbeeld bepaalde diensten af.

Met een protocol gebruik sociale media (en internet) kun je als school afspraken maken over het gebruik hiervan, zodat voor iedereen duidelijk is wat de regels zijn. Je kunt er voor kiezen om voor leerlingen andere afspraken te maken dan voor medewerkers. Een belangrijk punt hierbij is om te bepalen of medewerkers, die namens of voor de school communiceren, hun eigen sociale media-accounts mogen gebruiken.

Er is geen wettelijke verplichting om zo'n reglement of protocol te maken, maar het helpt wel om bewust om te gaan met sociale media binnen je school en draagt bij aan een sociaal veilig klimaat. Let

er wel op dat een protocol of reglement weer de instemming vereist van de (G)MR. Kennisnet helpt je op weg met een **modelreglement** (zie downloads verderop).

LET OP: De AVG stelt nieuwe eisen aan het gebruik van digitale diensten onder de 16 jaar. Wil je als school dat leerlingen *tijdens de les sociale media* gebruiken? Houd er dan rekening mee dat leerlingen jonger dan 16 jaar hiervoor de uitdrukkelijke toestenmming moeten krijgen van hun ouders/verzorgers.

- **Een bedrijf als facebook, of een aanbieder van een app, moet straks op zijn beurt (kunnen) controleren of de wettelijk vertegenwoordiger die toestemming echt heeft gegeven. De school moet dit kunnen aantonen. Deze regel kan gevolgen hebben voor de snelheid waarmee je als school gebruik kan maken van digitale diensten tijdens de lessen.**

Het is van belang om vooraf een goede afweging te maken over de inzet van sociale media in de lessen. Bedenk ook wat je doet als ouders géén toestemming geven (je wilt leerlingen niet uitsluiten van bepaalde lessen). Leg uit en leg vast wat de overweging is om sociale media in te zetten tijdens de les als digitaal lesmateriaal.

Meer informatie over sociale media vind je via onderstaande downloads Gebruik deze informatie om voor jouw school een duidelijk beleid rondom dit type media te formuleren. De volgende documenten kunnen helpen bij het maken van afspraken over sociale media bij jou op school.

Gedragscode ict en internetgebruik

Wettelijk gezien heb je als werkgever het recht om regels te stellen aan hoe iemand zijn werk moet doen, zolang maar duidelijk is welke regels je stelt en die regels binnen het redelijke blijven.

Zo is het verplicht om werknemers enige vrijheid te geven bij het privégebruik van internet en mail, maar men mag wel regels stellen over hoe dat privégebruik dan wordt uitgevoerd (“niet storend voor de dagelijkse werkzaamheden” is de standaardzin). Ook mag je een internetfilter instellen en niet-werk gerelateerde sites blokkeren. De regels moeten ook rekening houden met privacy, het bedrijfsbelang en ze moeten tegelijk algemeen genoeg zijn om alle situaties te dekken.

Veilig schoolklimaat en gedragscode

De overheid stimuleert een veilig schoolklimaat. Veiligheid heeft hierbij zowel betrekking op fysieke (o.a. brandveiligheid en letselveiligheid) als mentale aspecten (leerlingen en medewerkers moeten zich veilig en geborgen weten). Het Ministerie van Onderwijs adviseert scholen dan ook een gedragscode op te stellen.

De gedragscode ict en internetgebruik voor medewerkers en leerlingen geeft de kaders aan waarbinnen zowel medewerkers als leerlingen hun met name digitale werkzaamheden kunnen doen.

Let op: een gedragscode vereist de instemming van de (G)MR omdat het te maken heeft met de privacy van leerlingen en/of medewerkers.

We werken aan voorbeelden van gedragscodes voor leerlingen en medewerkers. De verwachting is dat deze begin maart 2018 in de Aanpak staan.

Monitoren

In hoeverre mag een school het internetverkeer of tabletgebruik van leerlingen en medewerkers volgen (‘monitoren’)? Mag de school zomaar toegang eisen tot een mailaccount van een leerling, of mag de directeur de e-mail van een zieke docent openen om een bericht van een ouder op te zoeken? De wet eist dat dit **vooraf** geregeld is en dat iedereen de afspraken kent.

Leg vast dat de medewekers van ICT-beheer niet zomaar e-mails mogen inzien: dat mag pas na toestemming van bijvoorbeeld het schoolbestuur of de directeur, en alleen als er twee personen meekijken (om te voorkomen dat men ‘uit interesse’ iets te enthousiast in de e-mail rondneust). Dergelijke afspraken kunnen meegenomen worden in de gedragscode.

TIP: Laat docenten in hun documenten of e-mailaccount een apart mapje aanmaken met de naam ‘privé’. Daarin staan documenten die niet werkgerelateerd zijn en waar collega's dus sowieso niet in mogen kijken.

Als het gaat over het **monitoren van devices van leerlingen**, dan spelen daar veel factoren een rol. Zie onderstaande download voor antwoorden op veelgestelde vragen over dit onderwerp.

Uitwisselen van gegevens

Passend onderwijs

Als leerlingen extra zorg of begeleiding nodig hebben, legt een school extra persoonsgegevens over de leerling vast, bijvoorbeeld over gezondheid of gedrag. Deze informatie ziet de wet als **bijzondere persoonsgegevens**. Een school moet extra zorgvuldig omgaan met deze gegevens.

Aparte afspraken

Op het moment dat de school gegevens wil uitwisselen met een andere organisatie, bijvoorbeeld een onderwijskundige, pedagoog of psycholoog, dan moet je daar **aparte afspraken** over maken. Deze afspraken leg je vast in een verwerkersovereenkomst waarin vertrouwelijkheid van de gegevens centraal staat. Let er ook op dat je bij het inschakelen van een externe deskundige zoals een psycholoog, ook de **toestemming** nodig hebt van de wettelijk verzorgers (ouders).

Soms lukt het niet om de juiste begeleiding op de school zelf te regelen. Dan schakel je het **samenwerkingsverband passend onderwijs**(afgekort: swv) in, bijvoorbeeld voor een toelaatbaarheidsverklaring passend onderwijs.

Swv

Het swv is een **zelfstandige organisatie**. De wet beschrijft dat het swv een zelfstandige wettelijke taak heeft. In privacytermen is het swv een ‘verwerkingsverantwoordelijke’, en dus zelf verantwoordelijk voor de gegevens van leerlingen. Zodra de school leerlinggegevens aanlevert aan het swv, is het swv verantwoordelijk voor de privacybescherming. Het swv is dus géén verwerker voor de school. Een schoolbestuur sluit dus géén verwerkersovereenkomst af met het swv. De wet regelt dat de school gegevens mag uitwisselen met het swv. De **vijf vuistregels** blijven uiteraard wél van toepassing.

Meer informatie over passend onderwijs is **hier** te vinden, of via de site van het steunpunt passend onderwijs van de VO-raad.

Jeugdhulpverlening

Het kan voorkomen dat een leerling extra ondersteuning nodig heeft, dat er thuis problemen zijn of dat een leerling met politie en justitie in aanraking is gekomen. In al deze gevallen wissel je gevoelige gegevens uit over leerlingen. Omdat de school gegevens uitwisselt met andere organisaties, moet duidelijk zijn hoe iedereen omgaat met de privacy van de leerlingen.

Basiszorg

De basiszorg voor jeugd en gezin is meestal per gemeente geregeld. Om gegevens met deze organisaties uit te kunnen wisselen is het belangrijk om afspraken te maken in een **convenant** (‘privacy convenant sociale wijkteams’), en om in een **privacyreglement** te beschrijven wat ieders rechten en

plichten zijn. Zie voor meer informatie het Convenant en privacy samenwerking jeugdhulpverleners.

Externe partners

Het Nederlands Jeugdinstituut heeft een handreiking gemaakt voor scholen die samenwerken met externe partners. Deze handreiking geeft informatie en praktische tips over hoe je om moet gaan met privacy en wat wel en niet mag binnen de kaders van de wet. Lees meer in de Handreiking samenwerking externe partners

Gezondheidsprojecten

Ook krijgen scholen regelmatig de vraag om mee te werken aan onderzoeken over de gezondheid van leerlingen. Wat er wel en niet mag bij deze gezondheidsprojecten lees je in Gegevensuitwisseling bij gezondheidsonderzoeken

Uitwisseling leerling dossiers en OKR

Om leerlingen zo goed mogelijk te begeleiden en het beste onderwijs te geven verzamelen scholen veel gegevens. Als een leerling overstapt naar een andere school, is het verplicht om informatie te delen met de nieuwe school. Met welke privacyaspecten moet de school dan rekening houden?

Primair onderwijs

Om ervoor te zorgen dat leerlingen in het basisonderwijs op hun nieuwe school de juiste ondersteuning en begeleiding krijgen, is in de 'Wet primair onderwijs' geregeld dat de basisschool de nieuwe school voorziet van een onderwijskundig rapport (**OKR**). Bij de overstap naar de middelbare school noemt men dit ook wel het **overstapdossier**. Na overleg met het onderwijzend personeel stelt de directie dit rapport op. Het rapport moet een goede, doorlopende leerlijn voor elke leerling garanderen.

Voor de uitwisseling van het OKR tussen de basisschool en de nieuwe school (po of vo), is geen toestemming van de ouders nodig. Ouders kunnen dan ook geen bezwaar maken tegen de uitwisseling van die informatie: de school moet de informatie hoe dan ook uitwisselen. Wel hebben ouders het recht op inzage van het overstapdossier, vóórdat deze wordt uitgewisseld. Inzage heeft geen aanpassing van het rapport tot gevolg. Bezwaren en opmerkingen van de ouders worden apart vastgelegd en toegevoegd aan het dossier. De school moet de mogelijkheid tot inzage van ouders schriftelijk vastleggen in het leerlingdossier. Hiermee maakt de school het controleerbaar dat de informatieplicht is nageleefd. Deze informatieplicht ligt immers wettelijk vast.

Voortgezet onderwijs

Ook de 'Wet voorgezet onderwijs' kent een overstapdossier. Het gaat daarbij om het contact met een andere school of instelling voor ander onderwijs, ten behoeve van de in- en uitschrijving van die leerling. Onder dit contact vallen alle uitwisselingen van leergegevens en de direct met het leren samenhangende begeleidingsgegevens.

Het uitgangspunt van het OKR is dat de scholen alleen gegevens overdragen die zij relevant vinden voor de nieuwe school.

De oude school mag dus niet het gehele leerlingdossier ongezien doorsturen, maar alleen die gegevens die nodig zijn om de leerling op de nieuwe school goed te begeleiden en te laten leren.

OSO

Uitgebreide informatie over de Overstapservice Onderwijs (OSO) en hoe privacy geregeld is vind je bij Overstapservice Onderwijs

Leerplicht en verzuim

Nederland is verdeeld in 39 Regionale Meld en Coördinatie punten (RMC) voor voortijdig schoolverlaters (vsv-ers). Elke RMC-regio heeft een contact-gemeente die de melding en registratie van voortijdige schoolverlaters coördineert en zorg draagt voor mogelijkheden van doorverwijzing en herplaatsing in het onderwijs.

Wat mag een leerplicht- / RMC-ambtenaar nu eigenlijk opvragen?

Belangrijk uitgangspunt bij het delen van informatie is:

- wat regelt de wet (grondslag)
- dataminimalisatie.

1. Leerplichtambtenaren hebben vanuit de Leerplichtwet een wettelijk recht op informatie, waarbij het vooral gaat om verzuiminformatie.
2. Een leerplichtambtenaar heeft alleen recht op die informatie die hij/zij strikt noodzakelijk nodig heeft voor de uitoefening van het werk. Een leerplichtambtenaar hoeft niet te zien dat een voorbeeldige leerling één uur mist…

Een leerplicht-/RMC-ambtenaar mag geen andere persoonsgegevens verwerken dan:

1. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens van de leerplichtige;
2. een administratienummer dat geen andere informatie bevat dan bedoeld onder a;
3. nationaliteit en geboorteplaats;
4. gegevens als bedoeld onder a, van de ouders, voogden of verzorgers van de leerplichtige;
5. gegevens met betrekking tot de inschrijving of afschrijving van de leerplichtige;
6. gegevens ten aanzien van het schoolverloop, het schoolverzuim en van het beroep op een vrijstelling van de leerplicht;
7. andere dan de onder a tot en met f bedoelde gegevens waarvan de verwerking is vereist ingevolge of noodzakelijk is met het oog op de toepassing van de Leerplichtwet 1969 of een andere wet.

Andere informatie delen mag niet. Een account in een leerlingvolgsysteem (Magister, Parnasys , SOMtoday enz) mag dan ook niet! (Daar mag een ambtenaar van gemeente of RMC zelfs niet eens om vragen!)

Wie mogen gegevens inzien?

Wie mogen eigenlijk de gegevens op school inzien? De vuistregel dataminimalisatie zegt het volgende:

- **Je gebuikt niet meer persoonsgegevens dan strikt noodzakelijk.**

- **Je zorgt er voor dat niet meer mensen toegang hebben tot die persoonsgegevens dan nodig is.**

Een conciërge zal niet altijd hoeven te weten welke leerlingen extra begeleiding nodig hebben, en de cijfers van wiskunde zijn niet altijd relevant voor een aardrijkskundedocent.

Dat betekent dat duidelijk moet zijn **'wie, wat, wanneer en waarom**' mag. Met een autorisatiematrix kun je een overzicht maken van wie, of welke rol, geautoriseerd is voor welke functie en wat die persoon wel of niet mag. De (informatie)systemen die de school gebruikt, moeten zijn ingericht op basis van deze rolverdeling.

Deze autorisatiematrix helpt scholen om de (informatie)systemen goed in te richten, en om te voorkomen dat 'iedereen overal zomaar bij kan en mag'.

2.c. Samen vooruit

De basis is nu op orde. We zijn aan de slag gegaan met IBP, we zijn goed op weg. Maar IBP is nooit af, we zullen regelmatig moeten evalueren en continue moeten verbeteren, we moeten nu groeien. Groeien in uitvoering van het beleid, maar ook groeien in het verder vereenvoudigen en waar nodig aanscherpen van de processen rondom IBP.

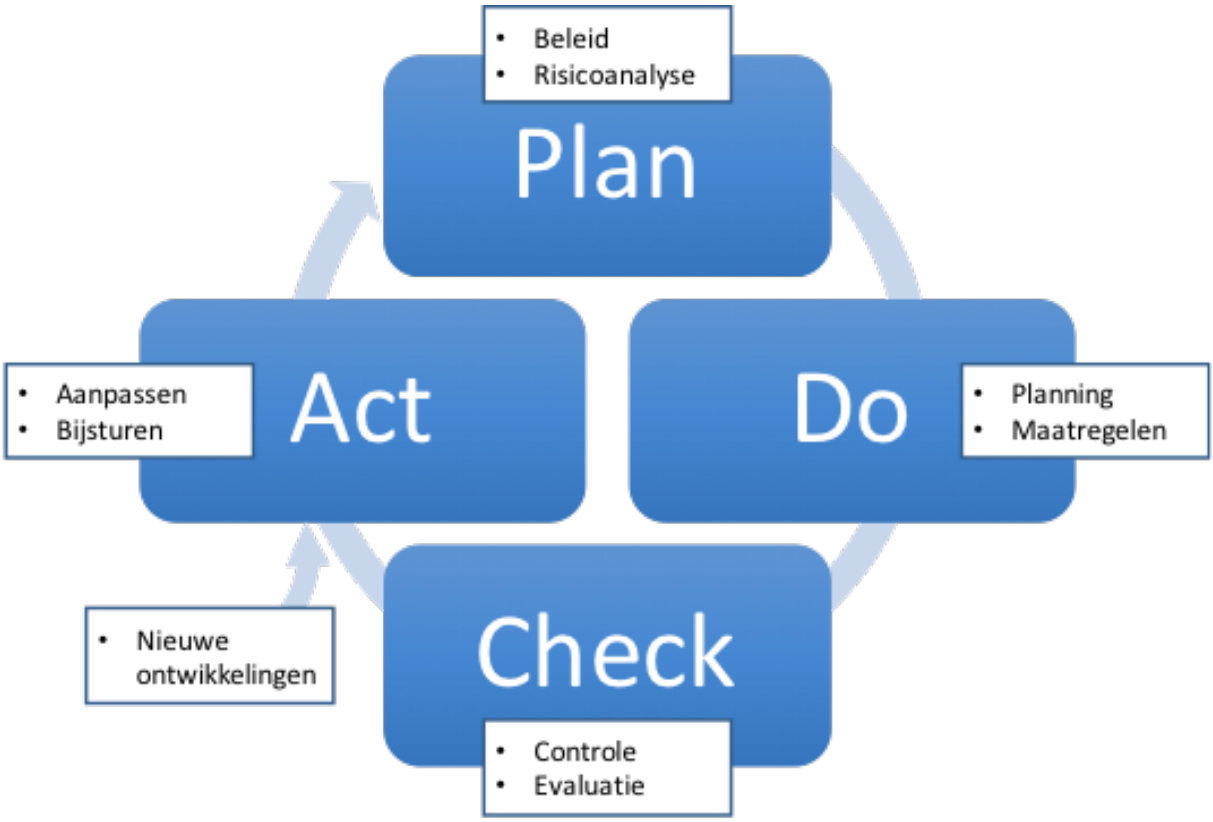
Kennisnet biedt je daar graag ondersteuning bij. We willen je dan ook vragen het IBP-beleid regelmatig intern te evalueren en eventuele aanvullende vragen aan Kennisnet voor te leggen. Op die manier kan deze online Aanpak steeds worden aangevuld met relevante onderwerpen, die mogelijk, ook op andere scholen spelen. Op die manier komen we samen vooruit.

Daarnaast zullen in deze module de grotere onderwerpen, die we samen op kunnen pakken, worden uitgewerkt. Zoals de gegevensbeschermingseffectbeoordeling, de documentatieplicht, DDoS en meer.

Evalueren en verbeteren

Om te kunnen groeien moet je continu kunnen verbeteren. Maar hoe pak je dat aan? Hoe weet je *wat* je moet verbeteren? Aanpassingen en verbeteringen komen onder andere naar voren bij het evalueren van IBP en de controle ervan. Maar ook kunnen ontwikkelingen zoals nieuwe processen of nieuwe systemen vragen om aanpassingen.

Continue verbeteren kun je organiseren op basis van Plan - Do - Check - Act, ofwel de **PDCA-cyclus**



Dit proces omvat vier stappen:

Stap 1. Plan

in deze stap formuleer je beleid ten aanzien van informatiebeveiliging en privacy. Je analyseert de bestaande situatie en brengt de kwaliteit van bestaande beveiligingsmaatregelen in beeld. Je kijkt welke bedreigingen onacceptabele risico's voor de organisatie vormen en wat het gewenste niveau van informatiebeveiliging is. Ook beschrijf je hoe de organisatie dit beleid ten uitvoer brengt.

IBP in Yucan:

- **Privacy-framework**
- **Proces-inventarisatie**
- **Registraties (verwerkingsregister) en compacte analyse processen en verwerkingen**
- **Eventueel uitvoeren (D)PIA's**
- **Privacy beleid**

Stap 2. Do

Tijd en middelen zijn beperkt, daarom maak je in deze stap een planning en een selectie van beveiligingsmaatregelen die het gewenste beveiligingsniveau dichterbij brengen. Ook voer je de maatregelen daadwerkelijk uit in de organisatie, applicaties en/of infrastructuur.

IBP in Yucan:

- **Beoordeling verbeterpunten via behandellijst**
- **Prioriteitstelling verbeterpunten**
- **Opstellen verbeterplannen**
- **Opstellen protocollen, procesbeschrijvingen etc.**

Stap 3. Check

Je beoordeelt alle activiteiten van het IBP-proces van de controle op naleving van het beleid, controle van de (voortgang van) de implementatie tot onafhankelijke controle.

IBP in Yucan:

- **Beoordeling of de geregistreerde processen en verwerkingen na actie voldoen, (status van de verbeterplannen?)**
- **Check op het Privacy-framework (is alles schoolbreed op orde?)**

Stap 4. Act

Daar waar nodig pas je bijvoorbeeld documenten, processen of maatregelen aan en kan bijsturing plaatsvinden van de planning of het beleid.

IBP in Yucan:

- **Bijstellen beleid**
- **Opstellen verbeterplannen**
- **Opstellen / bijstellen protocollen, procesbeschrijvingen etc.**

Ons advies is om deze cyclus **jaarlijks** terug te laten komen. Vanuit dit evaluatie proces kun je gewenste activiteiten in de kalender opnemen.

Functionaris voor Gegevensbescherming (FG)

Onder de AVG zijn onderwijsinstellingen, op grond van artikel 37-39, verplicht vanaf 25 mei 2018 een Functionaris voor Gegevensverwerking (FG) aan te stellen. Dit is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG

Wat is een FG?

Een Functionaris voor Gegevensverwerking (FG) is een interne toezichthouder op de verwerking van persoonsgegevens binnen een onderwijsinstelling. Deze functionaris heeft geen formele

sanctiebevoegdheden, maar wel controlebevoegdheden. Hij adviseert het schoolbestuur (bevoegd gezag) over privacy en houdt toezicht daarop, handelt vragen en klachten over privacy af, ontwikkelt (interne) regelingen rondom privacy en geeft advies over technologie en beveiliging (privacy by design). De FG moet voldoende kennis hebben van de organisatie en van privacywetgeving, betrouwbaar zijn en moet in onafhankelijkheid zijn werkzaamheden kunnen verrichten. De FG heeft de zelfde ontslagbescherming als leden van de (G)MR.

De verplichting om en FG aan te wijzen is één van de zaken die een schoolbestuur moet regelen vanaf 25 mei 2018. Niet alle schoolbesturen zullen dan al een FG hebben aangewezen, bijvoorbeeld omdat er nog afspraken moeten worden gemaakt met de schoolbesturen waarmee samen een FG wordt geregeld of omdat het schoolbestuur eerst de basis onder informatiebeveiliging en privacy wil hebben gelegd. Het advies is dat het schoolbestuur documenteert waarom er (nog) geen FG is aangewezen, en wat de planning is om dat wel te gaan doen. Het is verdedigbaar dat een schoolbestuur eerst andere verplichtingen uit de AVG op orde wil hebben gebracht voordat een FG daarop intern toezicht gaat houden.

Wat moet je doen?

In onderstaande 'Handreiking FG voor po/vo' wordt uitgelegd op welke grond een schoolbestuur een FG moet aanwijzen, hoe je die aanwijzing regelt, wat diens taken en bevoegdheden zijn en wat de functie-eisen zijn. Daarnaast worden een aantal praktijkvoorbeelden gegeven over hoe een FG geregeld kan worden.

IBP / FG in Yucan

In het privacy framework worden de vereisten uit de AVG die aan de functionalis gegevensbescherming worden gesteld behandeld (beleid, medewerkers). Je hebt de vereisten direct in beeld en kunt meteen een check doen of alles voldoet. Denk daarbij aan de kwalificaties maar ook hoe de school met de FG omgaat.

Gegevensbeschermings-effectbeoordeling (PIA)

De **Gegevensbeschermingseffectbeoordeling.** De AVG gebruikt hiervoor de termen ‘data protection impact assessment (DPIA) of PIA (Privacy Impact Assessment). Ook scholen zijn straks verplicht in bepaalde gevallen een zogenaamde “gegevensbeschermingseffectbeoordeling” te doen. Wanneer geldt die plicht? En hoe kun je dat als school oppakken.

Kennisnet heeft deze in voorbereiding; verwacht maart 2018. (*De vermelde datum is een indicatie, als daar wijzigingen in komen worden die hier ook weergegeven).*

IBP / (D)PIA in Yucan

In Yucan is de DPIA al voor u beschikbaar. Alle onderwerpen die aan de orde moeten komen zijn samen met ondersteunende informatie uit de wet en voorbeelden beschikbaar.

- **In de module kaarten start je een proces of verwerkingsregistratie.**
- **Je doet daar een korte check (o.a. op wetmatigheid).**

- **Als je verwacht dat er een aanmerkelijk risico is, start je daar de (D)PIA.**
- **Je volgt daarbij in het aangeboden format de wettelijk verplichte onderwerpen.**

- **Als er een risico beheersings maatregel moet worden genomen benoem je verbeterpunten.**
- **En in een verbeterproject definieer en plan je de maatregel.**
- **Je kunt het definieren en opvolgen aan een collega overdragen.**
- **Status en deadlines blijven in beeld en verantwoording is met een druk op de knop**

beschikbaar.

Documentatieplicht

De IBP gaat momenteel niet uitgebreid in op de documentatieplicht die vanuit de AVG wordt gesteld. De documentatieplicht is de onderlegger voor de verantwoordingsplicht. De verantwoordingsplicht onder de AVG is groot. De AP kan op ieder moment vragen om aan te tonen dat aan de eisen van de AVG wordt voldaan.

In het Privacy-framework komt alle vereiste documentatie aan de ordeDaarnaast zijn de in de module kaarten aangeboden formats (o.a. registraties, (D)PIA's, datalekken, etc) aangesloten op de inhoudelijke eisen die vanuit de AVG worden gesteld. En door de brede aanpak (van inventarisatie t/m verbeterplannen en privacyplannen) in Yucan te organiseren heeft u ook de verplichte verantwoording op de PDCA op de rit. En met een druk op de kno beschikbaar voor verslaglegging en verantwoording.

Dataregister (verwerkingsregister)

Onder de Wbp moesten scholen melding doen bij de Autoriteit Persoonsgegevens (AP) als zij persoonsgegevens gebruikten, die niet onder het vrijstellingsbesluit voor het onderwijs vielen. Met ingang van 25 mei 2018 vervalt niet alleen de Wbp, maar ook het vrijstellingsbesluit. Hiervoor komt de documentatieplicht of beter gezegd bewijsplicht in de plaats.

- **Alle verwerkingen van persoonsgegevens binnen of ten behoeve van de schoolorganisatie moet worden gedocumenteerd.**

IBP / Verwerkingsregister in Yucan

Als je start met de proces-inventarisatie zijn alle processen en verwerkingen binnen de school in beeld gebracht.

- Door deze in Yucan te registreren heeft de school haar verwerkingsregister volledig op de rit.
- De registraties volgen de vereiste onderwerpen uit de AVG. Je ziet direct wat moet worden vastgelegd.
- En er wordt per registratie de mogelijkheid geboden een compacte analyse op de wet uit te voeren.

- Als er een aanmerkelijk risico is geconstateerd of verwacht kan direct een (D)PIA's worden gestart.
- Ook de (D)PIA volgt en biedt de door de AVG vereiste onderwerpen met uitleg en voorbeelden.
- Ook worden aanwijzingen gegeven voor het eventueel aanvragen van een voorafgaande raadpleging.

d.d. 19 ferbuari 2018:

Kennisnet: Het dataregister voor medewerkers in vaste dienst en het register voor leerlingen zijn in de afrondende fase;

De verwachting is op dit moment dat deze eind februari gepubliceerd kunnen worden. (De vermelde datum is een indicatie, als daar wijzigingen in komen worden die hier ook weergegeven)

(D)DoS, wat moet ik weten...

en (D)Dos-aanval op school: dit kan iedereen overkomen. Je systemen liggen plat, je netwerk is traag en iedereen belt je met vragen. En jij vraagt je af: wat moet ik doen?

Wat is een DDoS-aanval?

Een (distributed) denial-of service of (D)DoS-aanval is één van de bedreigingen, die de continuïteit van het onderwijs steeds vaker in gevaar brengt. De aanval heeft als doel om de beschikbaarheid van een systeem te onderbreken. Het zorgt er bijvoorbeeld voor dat de website of de geplande digitale toets niet bereikbaar is. Dit gebeurt meestal door het versturen van meer verzoeken dan het systeem kan afhandelen. Wanneer een aanval vanaf meerdere computers (soms wel duizenden tegelijk) wordt uitgevoerd, dan is er sprake van een DDoS-aanval. Vaak wordt gebruik gemaakt van een zogenaamd botnet, een verzameling van computers die onder de controle van de aanvaller(s) zijn gekomen. Het is dan ook belangrijk om maatregelen tegen deze bedreiging te nemen, zodat het onderwijs door kan gaan.

DDoS-aanval op school: wat nu?

Het is niet eens de vraag of je als school te maken krijgt met een DDoS-aanval, maar meer wanneer. Wees er op voorbereid. Kennisnet heeft, in samenwerking met politie, scholen en leveranciers, een handig informatiedossier opgesteld over DDoS-aanvallen op school. In dit dossier vind je meer informatie over dit onderwerp.

Behalve informatie over DDoS-aanvallen, behandelt het ook de maatregelen die bestuurders, ict-coördinatoren en technisch medewerkers moeten nemen vooraf en tijdens een aanval. Zij zijn tenslotte samen verantwoordelijk voor de continuïteit van goed werkende en veilige ict-toepassingen op school. In de drie stappen herkennen, aanpak en preventie, wordt per takenpakket uitgelegd hoe jij jouw school zo goed mogelijk kan beschermen tegen DDoS-aanvallen en/of de gevolgen daarvan.

Bekijk het dossier DDoS-aanval op school

Cameratoezicht

Camera toezicht wordt vaak ingezet om veiligheid te waarborgen, maar hoe zit het met de privacy?Het inzetten van cameratoezicht past in een groter pakket aan fysieke maatregelen dat wordt toegepast om de veiligheid van medewerkers, leerlingen en bezoekers binnen en in de directe omgeving van locaties van po- en vo-instellingen te waarborgen.

Op po- en vo-instellingen hangen steeds vaker camera's. Bijvoorbeeld om vernielingen of diefstal tegen te gaan. Maar hiermee is de inbreuk op de privacy van leerlingen, medewerkers en bezoekers groot. Daarom mogen po- en vo-instellingen alleen camera's ophangen als zij aan een aantal voorwaarden voldoen. Ook moeten zij ervoor zorgen dat de inbreuk op de privacy zo klein mogelijk is. Een camera in bijvoorbeeld een toilet gaat te ver, omdat mensen dan ontkleed in beeld kunnen komen.

De handreiking cameratoezicht helpt po- en vo-instellingen om het gebruik van camera's goed te regelen, en daarbij de privacy van leerlingen, medewerkers en bezoekers te waarborgen. Het bijgesloten modelreglement cameratoezicht heeft betrekking op die locaties van een po- en vo-instelling, waar toezicht door middel van camerasystemen wordt ingezet. Het geeft een beschrijving van taken, verantwoordelijkheden en procedures over het cameratoezicht, met het oog op integer gebruik van het camerasysteem en de bescherming van privacy van leerlingen, medewerkers en bezoekers.

3. Communiceren

Waarom communiceren?

Mooi! Je ben bij de derde stap aangekomen. Nu moet je er voor zorgen dat IBP geen papieren tijger blijft, maar echt in de school gaat leven. Dat doe je door er over te **communiceren**.

Medewerkers

Vertel je medewerkers wat informatiebeveiliging voor hen betekent en hoe ze verstandig omgaan met persoonsgegevens. Hier zijn verschillende manieren voor om dit te bereiken. Het organiseren van een ‘security awareness training’ is een veelgebruikte methode om alle medewerkers te trainen in IBP.

Leerlingen

Aan je leerlingen leg je ook uit hoe je met hun gegevens omgaat. En hoe zij zélf verstandig omgaan met bijvoorbeeld hun schoolaccounts en wachtwoorden.

Ouders

En vergeet de ouders niet: zij beslissen over de privacy van hun kinderen (die jonger zijn dan 16 jaar). Ouders willen weten hoe IBP op jouw school geregeld is, zodat ze het vertrouwen krijgen dat de gegevens van hun kind bij jou veilig zijn.

Dialoog met medewerkers

Beleid en maatregelen zijn niet voldoende om risico’s op het gebied van informatiebeveiliging en privacy uit te sluiten. Meestal speelt de mens een belangrijke rol als er beveiligingsincidenten of datalekken zijn ontstaan. Daarom is het erg belangrijk om het bewustzijn bij de medewerkers te vergroten en aan te scherpen.

Bewustwording

Onderdeel van het IBP-beleid is dat je regelmatig terugkerende bewustwordingscampagnes voor medewerkers organiseert. Je kunt daarbij algemene scholing geven aan alle medewerkers, of specifieke trainingen organiseren voor groepen medewerkers die vaker met informatiebeveiliging en privacy te maken hebben. Denk bijvoorbeeld aan een bijeenkomst voor medewerkers van de administratie, of zorgcoördinatoren.

Elke medewerker en leerling moet er van uit kunnen dat er altijd zorgvuldig met zijn of haar persoonsgegevens wordt omgegaan. Naleving van de wetgeving is wel de verantwoordelijkheid van de bestuurder, maar naleving en borging hiervan kan alleen bereikt worden wanneer iedereen binnen de schoolorganisatie zorgvuldig en verantwoord met persoonsgegevens weten om te gaan.

Om dit te faciliteren zijn er twee mogelijkheden:

1. De eerste is een model PowerPointpresentatie. Een medewerker, die belast is met IBP, kan deze presentatie binnen zijn organisatie aan de medewerkers geven. Hij wordt hierbij ondersteunt door een inhoudelijke toelichting die in de notities van de slides zijn verwerkt.
2. Een tweede optie is dat medewerkers op eigen gelegenheid de online workshop "training bewustwording IBP voor medewerkers" in Wikiwijs doorlopen.

Klik voor de online workshop: "training bewustwording IBP voor medewerkers"

Of download verderop de presentie "IBP voor medewerkers".

Inhoudelijk komen de beide mogelijkheden overeen en wordt er ingegaan op hoe we met persoonsgegevens moeten omgegaan. Maar wat zijn nu precies persoonsgegevens? En wat betekent de wetgeving in de praktijk voor mij als medewerker in het primair- of het voortgezet onderwijs?

Onderstaande workshop geeft de mogelijkheid om kort en krachtig aan medewerkers op een deels

interactieve manier het belang van IBP te laten zien en aan te geven wat er gedaan kan en moet worden om de privacy van leerlingen en collega's te beschermen.

Aan het einde van de workshop kan iedere medewerker de onderstaande vragen kunnen beantwoorden:

- **Waarom** is IBP belangrijk?
- **Wat** zijn persoonsgegevens?
- **Waar** kan verantwoord met persoonsgegevens worden gewerkt?
- **Wanneer** mogen persoonsgegevens worden uitgewisseld?
- **Wie** is binnen de organisatie verantwoordelijk voor IBP?

Zie voor aanvullende informatie over informatiebeveiliging en privacy ook:

- de publicatie **ict-bekwaamheid van de leraar**
- de **do's en dont's van privacy.**

Dialoog met leerlingen

Ook leerlingen maken steeds meer gebruik maken van digitale middelen om te leren en te communiceren. Als je bedenkt dat 95% van de leerlingen in groep 8 een smartphone heeft en een groot deel actief is op sociale media, is het helemaal niet gek om in de klas het gesprek aan te gaan over hoe zij hun privacy kunnen bewaken. En hoe zij met de privacy van mede-leerlingen omgaan. Want mag je je wachtwoord met iemand delen? Maar ook; hoe gaan we met elkaar om op sociale media?

Naast slachtoffer op internet kunnen jongeren ook dader zijn. Door bijvoorbeeld het schoolwebsite te hacken of het systeem plat te leggen met een DDos-aanval. Wanneer er anti-pestregels zijn, anti-pestcontract of een gedragscode ict- en internetgebruik, wordt dit meestal klassikaal besproken. Maar hoe praat je nu eigenlijk in de klas over informatiebeveiliging en privacy?

Hoe ga je het gesprek aan met leerlingen over IBP?

Hiervoor hebben we 25 hulpvragen opgenomen om met leerlingen van 10- tot 18-jaar het gesprek aan te gaan over deze twee moeilijke onderwerpen. Zie onderop voor de downloads.

Digitale geletterdheid

21e eeuwse vaardigheden worden gezien als competenties die leerlingen nodig hebben in een snel veranderende maatschappij waarin technologie een belangrijke rol speelt. Onderdeel van die vaardigheden is het onderwerp digitale geletterdheid dat bestaat uit de 4 vaardigheden computational thinking, mediawijsheid, informatievaardigheden en ict-basisvaardigheden. Deze laatste vaardigheid gaat over het kennen van basisbegrippen en functies van computers en netwerken, het kunnen aansluiten en bedienen van hardware. Maar ook het kunnen omgaan met kantoortoepassingen, zoals tekstverwerkers en presentatiesoftware. En kunnen werken met internet, met mobiele apparaten en op de hoogte zijn van **beveiligings- en privacyaspecten.**

Meer informatie over digitale geletterdheid vind je hier:

https://www.kennisnet.nl/artikel/werken-aan-digitale-geletterdheid-zo-doe-je-dat/

Sociale media; maak iedereen mediawijs

We hebben gezien dat digitale geletterdheid ook inspeelt op beveiligings en privacy aspecten. Mediawijsheid omvat hier de kennis, vaardigheden en mentaliteit die nodig zijn om bewust, kritisch en actief om te gaan met media. Deze zijn onderverdeeld in:

- **Begrip**: inzicht hebben in de medialisering van de samenleving, begrijpen hoe media gemaakt worden, zien hoe media de werkelijkheid kleuren.

- **Gebruik**: apparaten, software en toepassingen gebruiken, je kunnen oriënteren binnen mediaomgevingen.
- **Communicatie**: informatie vinden en verwerken, content creëren, participeren in sociale netwerken.
- **Strategie**: reflecteren op het eigen mediagebruik, doelen realiseren met media.

Via onderstaande knoppen kun je nog meer informatie vinden over specifieke deelgebieden.

- **Mediawijsheid op de basisschool**
- **Social media in het speciaal onderwijs**
- **Onderzoek mediagebruik onder jongeren**
- **Workshop mediawijsheid**

Veilig online

Gebuik deze **filmpjes** van Alert Online om leerlingen te laten zien wat ze moeten doen om veilig online te zijn.

(D)Dos; Van kattenkwaad tot strafblad

Naast slachtoffer op internet kunnen jongeren ook dader zijn. Een (D)Dos-aanval op school, dat kan iedereen overkomen... Maar in de praktijk blijken de 'daders' vaak leerlingen te zijn, waarbij het uitvoeren van de (D)Dos-aanval als een grapje of middel om die digitale toets uit te stellen begint.

Het uitvoeren van een (D)Dos-aanval is strafbaar volgens de wet, met een maximale celstraf van 6 jaar. Bewustwording van de gevolgen van het uitvoeren van een (D)Dos-aanval en het hebben van een strafblad is belangrijk voor leerlingen. Je krijgt bijvoorbeeld geen baan bij de politie als je een strafblad hebt en ook is een baan als ethisch hacker niet waarschijnlijk. Praat hierover met de leerlingen en maak ze bewust van de gevolgen die dit soort grapjes kunnen hebben. Zie voor meer informatie over (D)DoS de rubriek (D)DoS, wat moet ik weten.

Leerlingraad

Voor een middelbare school zal een leerlingenraad een uitstekende gesprekspartner zijn om eens samen stil te staan bij privacy op school. Ga constructief het overleg in, leerlingen moeten ook leren dat hun gegevens het beschermen waard zijn. Als je als school het goede voorbeeld geeft, doet dat voorbeeld misschien wel goed volgen!

Dialoog met ouders

Scholen verzamelen en gebruiken steeds meer persoonsgegevens van en over leerlingen. Je bent wettelijk verplicht om te verantwoorden wat je met die gegevens doet. Ouders, en leerlingen (als zij 16 jaar en ouder zijn), hebben het recht om (ongevraagd) in begrijpelijke taal, uitgelegd te krijgen hoe privacy op jouw school is geregeld.

Zorg dat je als school vragen over privacy kan beantwoorden en hen uit kan leggen wat de school doet met de gegevens van hun kinderen. We beschrijven hier een aantal onderwerpen waar ouders regelmatig vragen over hebben.

Privacybijsluiter

Om uit te leggen welke afspraken je hebt gemaakt met uitgevers, distributeurs of leveranciers van software, kun je verwijzen naar de privacybijsluiter die bij de bewerkersovereenkomsten zit. In de privacybijsluiter vertelt de leverancier wat het product doet, welke gegevens hij gebruikt en wat het doel van dat gebruik is.

Wees transparant over privacy

Als ouders het vertrouwen hebben dat je IBP goed hebt geregeld, dan zullen ze veel sneller bereid zijn om gegevens te delen. Om je te helpen, zijn er een aantal voorbeeldteksten gemaakt die je kunt gebruiken in je schoolgids of voor op je website. Zie onderop voor de download.

Filmen en fotograferen door ouders

De school maakt afspraken over het gebruik van foto's van leerlingen voor de website, schoolgids enz. Ouders moeten hiervoor specifiek toestemming geven en bezwaar kunnen maken als zij niet willen dat een foto van hun kind hiervoor gebruikt wordt.

Maar wat doe je met ouders die op school foto's maken? Hoe ga je om als ouders foto's van de beveiligde site kopiëren en vervolgens delen? Het is aan de school hoe zij hiermee omgaan. Verbieden is lastig, maar afspraken maken kan een oplossing zijn. Onderop vind je een download met enkele voorbeeldafspraken.

Wat is de rol van de (G)MR rondom privacy?

Het is verstandig om ook jaarlijks met de (G)MR te praten over hoe jouw school omgaat met leerlinggegevens. Openheid en transparantie over het gebruik van leerlinggegevens is het uitgangspunt in alle communicatie met ouders! De MR heeft ook instemmingsrecht als het gaat over onderwerpen waarbij privacy van leerlingen en medewerkers een rol spelen. Zo moet het privacyreglement worden goedgekeurd door de (P)MR.

Mogen grootouders en pleegouders ook vragen om inzage?

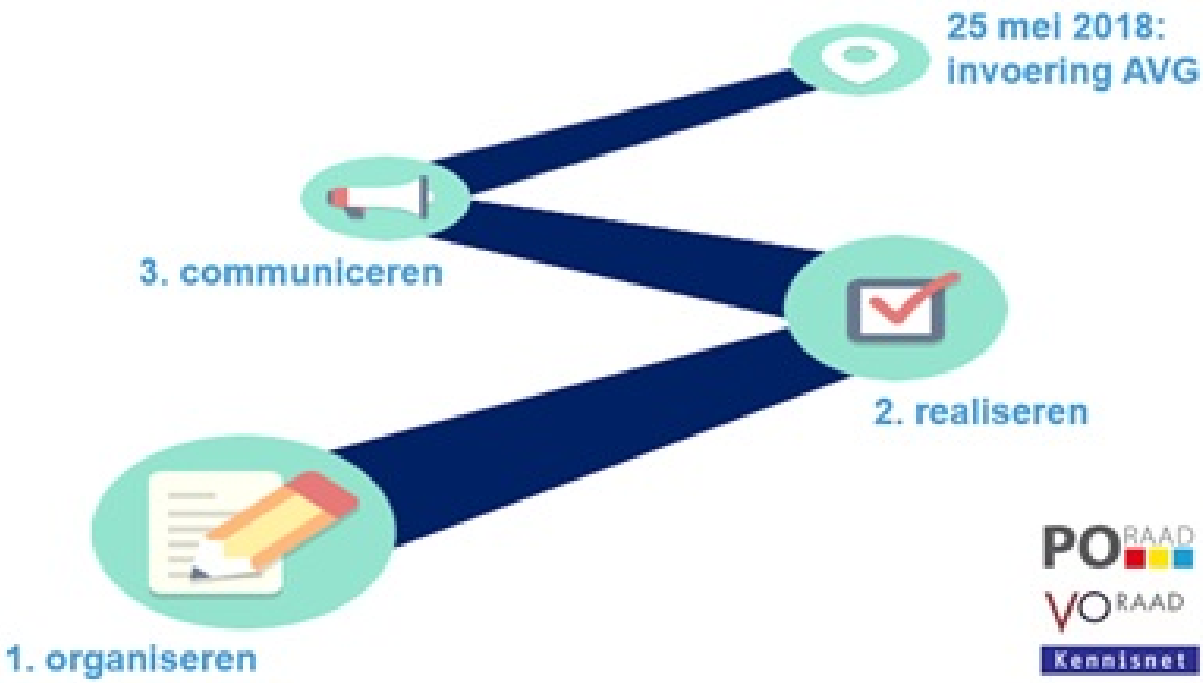
Bij leerlingen onder de 16 jaar heeft de wettelijk vertegenwoordiger het gezag over het kind en beslist namens het kind over de privacy. Dat zullen in de meeste gevallen één of beide ouders zijn. Maar ook pleegouders, die officieel het gezag over het kind hebben, hebben recht op inzage van het dossier. Grootouders mogen het dossier van hun kleinkind niet inzien. Dat ligt anders, zij zullen niet snel de wettelijk vertegenwoordiger zijn.

Hoe ver ben je met de IBP?

Heb je alle stappen uitgevoerd?

Prima, je bent goed bezig om informatiebeveiliging en privacy te regelen!

Door bewust en zorgvuldig om te gaan met leerlinggegevens is jouw school er klaar voor om deze gegevens nóg beter en efficiënter in te zetten. Informatiebeveiliging of privacy zijn geen bedreiging meer. Gepersonaliseerd leren met ict? Kom maar op!



Maar... Hoe ver ben jij eigenlijk?

Hoe ver ben je nu met jouw school? Ben je net aan de slag gegaan, al goed op weg of werk je aan 'samen vooruit'? En ben je nu klaar?

Informatiebeveiliging en privacy kun je niet in één keer regelen het is een *proces*. **Met deze 'Aanpak IBP' heb je de belangrijkste risico's en maatregelen in beeld. Als je alle maatregelen uit de aanpak hebt ingevoerd ben je aardig 'in control'**.

Met de praktische checklist IBP in het Privacy Framework kun je controleren hoe ver je daadwerkelijk bent met het regelen van je IBP. Het geeft een snel en praktisch overzicht van wat er uit de IBP gereed is en wat je op de planning hebt staan. Bekijk de checklist in samenhang met het gehele privacy-framework!

IBP is nooit af...

Heb je alle stappen doorlopen en denk je dat je klaar bent? Mooi! Maar eigenlijk ben je niet klaar. Bij Kennisnet zeggen we wel eens dat het échte werk pas begint als je de Aanpak IBP doorlopen hebt! Alle genomen maatregelen en afspraken moeten nog worden getoetst op de wet en worden nu in de praktijk gebracht. Er moet gekeken worden hoe het in de dagelijkse praktijk gaat werken. En volgend jaar komt de risicoanalyse weer terug met misschien wel nieuwe risico's en uitdagingen die opgelost moeten worden. De PDCA-cyclus gaat zijn werk dus doen!

Het regelen van IBP is iets dat elke organisatie in Europa moet doen. Er voor zorgen dat je 'aantoonbaar compliant' bent met wet- en regelgeving doe je voor jezelf! Elke organisatie heeft zo zijn eigen risico's in beeld en weet wat hem te doen staat om IBP goed te regelen. Je bent dus niet de enige school, ook scholen in Duitsland, Polen, Spanje, Portugal, enzovoorts moeten IBP regelen.

De Aanpak is gebaseerd op de wetteksten van AVG en Wbp, daarnaast bevat het een groot aantal onderdelen vanuit de informatiebeveiliging, dus vanuit de ISO27001/2-normen. Verder zijn de maatregelen gebaseerd op het framework IBP voor het mbo, dat weer is gebaseerd op het normenkader informatiebeveiliging zoals dat in het hoger onderwijs wordt toegepast. **Let op dat de AVG inhoudelijk meer vereist dan in de IBP langskomt. De IBP voor elkaar hebben is wel een belangrijk onderdeel daarvan. Doorloop ter controle het Privacy-Framework.**

En nee, na het doorlopen van de Aanpak IBP is er geen certificaat om aan de muur te hangen. Wel heb je een overzicht voor jezelf, je bestuurder en de toezichthouders van wat er allemaal geregeld is, wat er nog op de planning staat en dat je het jaarlijks evalueert en werk aan bewustwording bij medewerkers, leerlingen en ouders.

En het is ook niet niks wat je gedaan hebt … onderwijs met inzet van ict kan op jouw school altijd doorgaan en je hebt de privacy van leerlingen, hun ouders en medewerkers geregeld!

III. Proces-Inventarisatie

Aandachtsgebieden

De onderstaande aandachtsgebieden kunnen afdelingen zijn of gegroepeerde activiteiten of verantwoordelijkheden op het genoemde gebied.

Processen kunnen een enkele bewerking van persoonsgegevens bevatten of een aantal verschillende bewerkingen die in de samenhang van een proces of activiteit bestaan. Zie ook de gegeven voorbeelden bij ieder aandachtsgebied.

(AVG: Artikel 4, lid 1) Persoonsgegevens: Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (AVG: De betrokkene):

Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens (denk aan woonadres, postcode en woonplaats), een online identificator (denk ook aan e-mailadres, inlognaam, gebruikersnaam) of één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Leiding

Directie

Management

Externe relaties

Werving & Communicatie

Op het gebied van werving & communicatie bestaan processen waarin persoonsgegevens worden verwerkt (verzamelen, bewaren, gebruiken, verstrekken in brede zin, zowel digitaal als fysiek).

Toelichting

Bijvoorbeeld: ontwikkelen schoolgids, posters, materialen waar beeldmateriaal van leerlingen wordt gebruikt, versturen van mailingen, nieuwsbrieven, contactformulieren op uw website, online en hardcopy inschrijfformulieren, online enquetes, online inschrijfformulieren, tracking van gebruikers van uw website, bezoekersstatistieken, bewaren en gebruiken van gegevens van mogelijke nieuwe leerlingen, organisatie evenementen, beheer opvolging wettelijke vereisten t.a.v. transparantie naar en uitoefening van rechten door betrokkenen.

Als u deze activiteiten binnen de organisatie uitvoert dan bent u de gegevensverantwoordelijke. Heeft u deze activiteiten uitbesteed dan bepaalt u de doeleinden en middelen en blijft u de gegevensverantwoordelijke. De organisatie aan wie het hebt uitbesteed is de verwerker waarmee u

een verwerkingsovereenkomst dient af te sluiten.

Inventariseer en benoem de processen en geef aan of - en zo ja - in welke rol de organisatie binnen dit aandachtsgebied persoonsgegevens verwerkt. U kunt onderscheid maken tussen gegevensverantwoordelijke (u bepaalt de doeleinden en middelen voor de verwerking), u bent gegevensverantwoordelijke maar hebt het proces of de verwerking uitbesteed, u bent de verwerker (u verwerkt de persoonsgegevens in opdracht van een gegevensverantwoordelijke en bepaalt de doeleinden en middelen niet) of sub-verwerker (u verwerkt persoonsgegevens in opdracht van een verwerker).

Inkoop

Samenwerkingen

Onderwijs

Lesgeven

Op het gebied van lesgeven bestaan processen waarin persoonsgegevens worden verwerkt (verzamelen, bewaren, gebruiken, verstrekken in brede zin, zowel digitaal als fysiek).

Toelichting

Bijvoorbeeld: Adres- en contactgegevens van leerlingen, absentieregistratie, digitale tools in en buiten de klas, lerarenvergaderingen, samenwerkingen met pedagogen of specialisten tbv een leerling, het rekening houden met specifieke kenmerken (bv. ADHD) van leerlingen, opvolging wettelijke vereisten.

Als u deze activiteiten binnen de organisatie uitvoert dan bent u de gegevensverantwoordelijke. Heeft u deze activiteiten uitbesteed dan bepaalt u de doeleinden en middelen en blijft u de gegevensverantwoordelijke. De organisatie aan wie het hebt uitbesteed is de verwerker waarmee u een verwerkingsovereenkomst dient af te sluiten.

Inventariseer en benoem de processen en geef aan of - en zo ja - in welke rol de organisatie binnen dit aandachtsgebied persoonsgegevens verwerkt. U kunt onderscheid maken tussen gegevensverantwoordelijke (u bepaalt de doeleinden en middelen voor de verwerking), u bent gegevensverantwoordelijke maar hebt het proces of de verwerking uitbesteed, u bent de verwerker (u verwerkt de persoonsgegevens in opdracht van een gegevensverantwoordelijke en bepaalt de doeleinden en middelen niet) of sub-verwerker (u verwerkt persoonsgegevens in opdracht van een verwerker).

Examinering

Leerlingvolgsystemen en leerlingdossiers

In en rondom leerlingvolgsystemen en leerlingdossiers bestaan processen en activiteiten waarin persoonsgegevens worden verwerkt (verzamelen, bewaren, gebruiken, verstrekken in brede zin, zowel digitaal als fysiek).

Toelichting

Als u deze activiteiten en processen binnen de organisatie uitvoert dan bent u de gegevensverantwoordelijke. Heeft u deze activiteiten of processen uitbesteed dan bepaalt u de doeleinden en middelen en blijft u de gegevensverantwoordelijke. De organisatie aan wie het hebt uitbesteed is de verwerker waarmee u een verwerkingsovereenkomst dient af te sluiten.

Inventariseer en benoem de processen en geef aan of - en zo ja - in welke rol de organisatie binnen dit aandachtsgebied persoonsgegevens verwerkt. U kunt onderscheid maken tussen gegevensverantwoordelijke (u bepaalt de doeleinden en middelen voor de verwerking), u bent gegevensverantwoordelijke maar hebt het proces of de verwerking uitbesteed, u bent de verwerker (u verwerkt de persoonsgegevens in opdracht van een gegevensverantwoordelijke en bepaalt de doeleinden en middelen niet) of sub-verwerker (u verwerkt persoonsgegevens in opdracht van een verwerker).

Schoolprojecten

Ondersteunend

Leerlingen- en algemene administratie

Op het gebied van leerlingen en algemene ondersteuning bestaan processen waarin persoonsgegevens worden verwerkt (verzamelen, bewaren, gebruiken, verstrekken in brede zin, zowel digitaal als fysiek).

Toelichting

Bijvoorbeeld: absentiemeldingen leerlingen en docenten, verwerken van leerlinggegevens, verwerking aanmeldingen en vertrek, leerlingendossiers, inzage in leerlingvolgsystemen, het verzorgen van een mailing, verwerking online aanmeldformulieren, enquetes en inschrijfformulieren, binnenkomende C.V's en motivatiebrieven in wervingsprocedures, verslagen van functioneringsgesprekken, in- en uitdienstprocessen, toegangsbeheer voor gebouwen klachtafhandeling, opvolging wettelijke vereisten.

Als u deze activiteiten binnen de organisatie uitvoert dan bent u de gegevensverantwoordelijke. Heeft u deze activiteiten uitbesteed dan bepaalt u de doeleinden en middelen en blijft u de gegevensverantwoordelijke. De organisatie aan wie het hebt uitbesteed is de verwerker waarmee u een verwerkingsovereenkomst dient af te sluiten.

Inventariseer en benoem de processen en geef aan of - en zo ja - in welke rol de organisatie binnen dit aandachtsgebied persoonsgegevens verwerkt. U kunt onderscheid maken tussen gegevensverantwoordelijke (u bepaalt de doeleinden en middelen voor de verwerking), u bent gegevensverantwoordelijke maar hebt het proces of de verwerking uitbesteed, u bent de verwerker (u verwerkt de persoonsgegevens in opdracht van een gegevensverantwoordelijke en bepaalt de doeleinden en middelen niet) of sub-verwerker (u verwerkt persoonsgegevens in opdracht van een verwerker).

financiële dienstenen administratie, salarisadministratie

personeelszaken (HR)

Op het gebied van personeelszaken bestaan processen waarin persoonsgegevens worden verwerkt (verzamelen, bewaren, gebruiken, verstrekken in brede zin, zowel digitaal als fysiek).

Toelichting

Bijvoorbeeld: Beoordeling van C.V's en motivatiebrieven in wervingsprocedures, functioneringsgesprekken, in- en uitdienstprocessen, inzet invalkrachten, flexwerkers of ZZP'ers (zijn juridisch mogelijk gegevensverwerkers), gedrags- en competentiemetingen t.b.v. ontwikkeling medewerkers al dan niet uitgevoerd door HR of externen, opvolging ziekmeldingen en ARBO gerelateerde processen, klachtafhandeling, opvolging wettelijke vereisten.

Als u deze activiteiten binnen de organisatie uitvoert dan bent u de gegevensverantwoordelijke. Heeft u deze activiteiten uitbesteed dan bepaalt u de doeleinden en middelen en blijft u de gegevensverantwoordelijke. De organisatie aan wie het hebt uitbesteed is de verwerker waarmee u een verwerkingsovereenkomst dient af te sluiten.

Inventariseer en benoem de processen en geef aan of - en zo ja - in welke rol de organisatie binnen dit aandachtsgebied persoonsgegevens verwerkt. U kunt onderscheid maken tussen gegevensverantwoordelijke (u bepaalt de doeleinden en middelen voor de verwerking), u bent gegevensverantwoordelijke maar hebt het proces of de verwerking uitbesteed, u bent de verwerker (u verwerkt de persoonsgegevens in opdracht van een gegevensverantwoordelijke en bepaalt de doeleinden en middelen niet) of sub-verwerker (u verwerkt persoonsgegevens in opdracht van een verwerker).

gebouwen en faciliteiten

ICT services en informatiemanagement

juridische zaken

kwaliteitsmanagement en compliance

Kennis & ontwikkeling

Kennis & ontwikkeling

Overig

Overig

IV. Privacy Framework

De onderwerpen, aspecten en toelichtingen in het privacy framework beslaan de relevante aandachtspunten voor privacymanagement in de organisatie. Het doorlopen van deze onderwerpen helpt u bij het inzichtelijk maken en houden van de status van het privacybeleid, de uitvoering daarvan en het voldoen aan wet- en regelgeving. Het geheel biedt een krachtig instrument om over het geheel van verplichtingen 'in control' te zijn en te voldoen aan de vereisten van de AVG.

Daaraan voorafgaand de **praktische checklist IBP**. Deze geeft een compact beeld van de mate waarin de aandachtspunten, onderwerpen en acties uit de IBP zijn ingevuld.

- Praktische checklist IBP

Hoe ver ben je met de IBP?

Hoe ver ben je nu met jouw school? Ben je net aan de slag gegaan, al goed op weg of werk je aan 'samen vooruit'? En ben je nu klaar?

Informatiebeveiliging en privacy kun je niet in één keer regelen het is een *proces*. Het belangrijkste is dat je *begint* om IBP te regelen, zodat ook jouw school straks gereed is voor de AVG in mei 2018. **Met deze ‘Aanpak IBP’ heb je de belangrijkste risico’s en maatregelen in beeld. Als je alle maatregelen uit de aanpak hebt ingevoerd ben je aardig ‘in control’.**

Zoals al eerder gezegd is IBP een *proces.* Het is nooit ‘af’. Door vooruit te kijken kun je rekening houden met risico’s die er nu nog niet zijn, maar wel gaan komen. Daarmee ben je klaar voor de toekomst en kun je vol vertrouwen gebruik maken van (nieuwe) ict-toepassingen zonder bang te zijn voor datalekken of misbruik van persoonsgegevens.

Met de praktische checklist IBP op de volgende pagina's kun je controleren hoe ver je daadwerkelijk bent met het regelen van je IBP. Het geeft een snel en praktisch overzicht van wat er uit de IBP gereed is en wat je op de planning hebt staan.

Per punt in de checklist worden daarbij relevante delen in het verdere privacy framework aangestipt (*.*).

Let op!

- **Met het op orde hebben van de checklist voldoe je niet op voorhand aan de eisen van de AVG. Wel heb je een goed beeld van de acties die in de IBP zijn langsgekomen en een belangrijk deel doorlopen.**
- **De AVG stelt meer en op punten specifieker eisen. Controleer of dat wat je hebt gerealiseerd voldoet, door het hele Privacy-framework te doorlopen.**

1. Organiseren

De aandachtspunten, onderwerpen en acties uit het onderdeel 'Organiseren' zijn ingevuld.

Toelichting

De per aspect tussen haken weergegeven nummering verwijst naar de onderwerpen in deel 1 t/m 7 van het Privacy-framework.

	NIET	BEPERKT	GROTENDEELS	GEHEEL	NIET VAN TOEPASSING
a De medewerkers weten waar de IBP over gaat. Zij zijn bekend met de basisbegrippen, de aandachtspunten AVG en de 5 vuistregels (1.1, 1.2, 2.1).					
b De bestuurder weet waarom een privacy-beleidsplan nodig is (1.1, 1.2).					
c. De bestuurder weet wat de AVG voor hem of haar als bestuurder inhoudt (1.1, 1.2).					
d. Het IBP-beleid is opgesteld, vastgesteld door het schoolbestuur en gecommuniceerd met betrokkenen (1.1, 1.2).					
e. De IBP-organisatie is ingericht (taken en rollen) waarbij verantwoordelijkheden en taken zijn belegd bij medewerkers (1.2, 2.1, 2.2).					
f. Privacyreglement is vastgesteld (let op: instemming (P)MR) en gecommuniceerd met betrokkenen (1.1).					
g. Basismaatregelen IBP en toegangsbeleid gegevens en applicaties zijn goedgekeurd en vastgelegd (5.3)					
h. De Functionaris voor de Gegevensbescherming is benoemd (2.3)					
i. Reglement Functionaris voor Gegevensbescherming is vastgesteld (1.1, 2.3)					
j. Evalueren toepassing en werking IBP-beleid op basis van rapportages. PDCA-cyclus (1.1, 1.2, 1.3)					
k.* Conclusie:					

2. Realiseren

De aandachtspunten, onderwerpen en acties uit het onderdeel 'Realiseren' zijn ingevuld.

Toelichting

De per aspect tussen haken weergegeven nummering verwijst naar de onderwerpen in deel 1 t/m 7 van het Privacy-framework.

	NIET	BEPERKT	GROTENDEELS	GEHEEL	NIET VAN TOEPASSING
a IBP-verantwoordelijke en proces-eigenaren weten wat de achtergrond van de te realiseren maatregelen zijn (6.1, 6.2, 6.3).					
b IBP-verantwoordelijke en proces-eigenaren hebben gegevens en processen geclassificeerd (6.1, 6.2, 6.3).					
c. IBP-verantwoordelijke en met proces-eigenaren hebben de huidige situatie in beeld gebracht en een Risicoanalyse gedaan. (6.1, 6.2, 6.3).					
d. IBP-verantwoordelijke en proces-eigenaren hebben op basis van de risicoanalyse de belangrijkste te nemen maatregelen bepaald en vastgesteld (6.1, 6.2, 6.3).					
e. IBP-verantwoordelijke en proces-eigenaren hebben een planning gemaakt van de actiepunten (activiteitenplanning) (6.1, 6.2, 6.3).					
f. IBP-verantwoordelijke en proces-eigenaren hebben verbetervoorstellen IBP in de planning opgenomen (6.1, 6.2, 6.3).					
I.* Conclusie:					

2.a Aan de slag

De aandachtspunten, onderwerpen en acties uit het onderdeel 'Aan de slag' zijn ingevuld.

Toelichting

De per aspect tussen haken weergegeven nummering verwijst naar de onderwerpen in deel 1 t/m 7 van het Privacy-framework.

	NIET	BEPERKT	GROTENDEELS	GEHEEL	NIET VAN TOEPASSING
a Er is een Procedure melden beveiligingsincidenten (datalekken) opgesteld, goedgekeurd en gecommuniceerd (6.4).					
b Er is een meldpunt datalekken en beveiligingsincidenten dat bij iedereen bekend is (6.4).					
c. Incidentenregistratie is ingeregeld (6.4).					
d. Rechten betrokkenen zijn vastgelegd en gecommuniceerd naar medewerkers, leerlingen en ouders (7.4 t/m 7.10)					
e. Er is een procesbeschrijving hoe betrokkenen hun rechten kunnen uitoefenen (7.4 t/m 7.10)					
f. Privacyreglement is gemaakt, vastgesteld door bestuurder en gecommuniceerd (1.1, 1.2).					
g. Er is een geheimhoudingsovereenkomst voor medewerkers niet in vaste dienst (2.1, 2.2)					
h. Er is een wachtwoordbeleid (5.3)					
i. Er is een Responsible disclosure (5.3)					
j. Er zijn afspraken gemaakt met leveranciers, die persoonsgegevens verwerken (beheer en toetsing contracten) Verwerkersovereenkomsten (3.1).					
k. De Privacy bijsluiter van de verwerkers-overeenkomsten zijn gepubliceerd (transparantie) (3.1, 7.1, 7.2).					
l. Toestemming ouders/leerlingen voor gebruik beeldmateriaal is geregeld (5.1, 6.2, 7.1, t/m 7.10)					
m. Procedure om toestemming in te trekken is vastgelegd en gecommuniceerd ((7.1 t/m 7.10)					
n. Afspraken en procedures over privacy zijn geregeld en gecommuniceerd (informatieplicht, transparantie) (7.1 t/m 7.10)					
o. Processen rondom Informatieplicht zijn ingericht (7.1 t/m 7.10)					
p.* Conclusie:					

2.b Goed op weg

2.c Samen vooruit

3. Communiceren

1. Management & Beleid

De met een (*) gemarkeerde onderwerpen en aspecten zijn vereisten van de AVG.

Indien onderwerpen of aspecten naar uw inzicht niet van toepassing zijn voor uw organisatie, dan is het raadzaam in ieder geval te overwegen of en zo ja; hoe deze van invloed zijn op het privacybeschermingsniveau en het voldoen aan wet- en regelgeving.

1.1* Privacybeleid

De organisatie heeft een adequaat privacybeleid vastgesteld.

Toelichting

Een adequaat en bij de organisatie passend privacybeleid is wettelijk verplicht (AVG) en helpt de organisatie grip te krijgen en houden op privacy gerelateerde zaken en de bescherming daarvan. Inzicht in risico's, het formuleren van een visie en het vaststellen hoe de organisatie waarborgt dat gegevens rechtmatig, behoorlijk en transparant verwerkt, zijn de onderleggers voor een bestendige en gedragen implementatie en borging van adequate privacybescherming.

Uit Checklist IBP:

- De medewerkers weten waar de IBP over gaat. Zij zijn bekend met de basisbegrippen, de aandachtspunten AVG en de 5 vuistregels.
- De bestuurder weet waarom een privacy-beleidsplan nodig is.
- De bestuurder weet wat de AVG voor hem of haar als bestuurder inhoudt.
- Het IBP-beleid is opgesteld, vastgesteld door het schoolbestuur en gecommuniceerd met betrokkenen.
- Privacyreglement is vastgesteld (let op: instemming (P)MR) en gecommuniceerd met betrokkenen.
- Reglement Functionaris voor Gegevensbescherming is vastgesteld.
- Evalueren toepassing en werking IBP-beleid op basis van rapportages. PDCA-cyclus.
- Privacyreglement is gemaakt, vastgesteld door bestuurder en gecommuniceerd.
- Security awareness training is gegeven aan alle medewerkers.
- Er wordt aandacht geschonken aan ict-bekwaamheid leraar.
- Leerlingen zijn geïnformeerd over IBP op school.
- Er wordt aandacht geschonken aan mediawijsheid en digitale geletterdheid van leerlingen.
- De leerlingenraad wordt bij IBP betrokken.
- Privacyreglement is gecommuniceerd en opgenomen op website en/of in schoolgids.
- Sociale-mediareglement is bekend gemaakt aan alle betrokkenen.
- Gedragscode ict- en internetgebruik is bekend gemaakt aan alle betrokkenen.
- Ouders worden actief benaderd en geïnformeerd over IBP op school en gewezen op hun rechten.
- De (G)MR is (wordt regelmatig) geïnformeerd over IBP op school.

	VOLDOET NIET	VOLDOET BEPERKT	VOLDOET GROTENDEELS	VOLDOET GEHEEL	NIET VAN TOEPASSING
a.* De organisatie heeft een overkoepelend privacybeleid vastgesteld en goedgekeurd waaruit blijkt dat zij kennis heeft en zich bewust is van haar risico's en wetgeving ten aanzien van privacybescherming en waarin haar visie op privacybescherming is beschreven.					

b.* In het privacybeleid is beschreven hoe zij waarborgt hoe de organisatie gegevens verwerkt en hoe zij zich aan wet- en regelgeving houdt, waarin uitdrukkelijk doch niet uitsluitend wordt voldaan aan de beginselen van rechtmatigheid, behoorlijkheid, transparantie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en verantwoordingsplicht zoals de AVG dat vereist.					
c. Het privacybeleid bevat effectieve bevoegdheden, taakstelling en afspraken over de verantwoordelijkheden en inbreng van de eindverantwoordelijke voor privacy.					
d. Het privacybeleid bevat effectieve bevoegdheden, taakstelling en afspraken over de verantwoordelijkheden en inbreng van toezichthouders.					
e.* Het privacybeleid is beschikbaar begrijpelijk voor (proces-) verantwoordelijken en uitvoerders en omschrijft minimaal richtlijnen voor en wettelijke eisen, waaraan processen, bepalingen, werkafspraken, communicatie en medewerkers ten aanzien van privacy en privacy gerelateerde zaken en situaties moeten voldoen.					
f.* Het privacybeleid of minimaal de voor de betrokkenen relevante delen daarvan zijn beschikbaar en begrijpelijk voor betrokkenen (wiens persoonsgegevens worden verwerkt) en beschrijft de wijze waarop wordt gewaarborgd dat hun rechten worden beschermd en hen voldoende ruimte wordt geboden voor uitoefening daarvan.					
g.* Het privacybeleid bevat onderwerpen, procedures en frequenties voor adequate evaluatie van doelmatigheid en doeltreffendheid op het gebied van privacybescherming en de naleving van privacyregelgeving.					
h. Het privacybeleid is zodanig concreet dat de effectiviteit kan worden gemeten, gecontroleerd en privacybescherming gericht kan worden geoptimaliseerd.					
I.* Conclusie:					

1.2* Privacymanagement

1.3* Compliance & PDCA

2. Medewerkers

De met een (*) gemarkeerde onderwerpen en aspecten zijn vereisten van de AVG.

Indien onderwerpen of aspecten naar uw inzicht niet van toepassing zijn voor uw organisatie, dan is het raadzaam in ieder geval te overwegen of en zo ja; hoe deze van invloed zijn op het privacybeschermingsniveau en het voldoen aan wet- en regelgeving.

2.1* Proceseigenaren & uitvoerders

Proceseigenaren en uitvoerders voldoen aan de taakstelling en vereisten van het privacybeleid.

Toelichting

Onder proceseigenaren en uitvoerders worden de personen in de organisatie verstaan die verantwoording dragen voor een proces en/of handeling waarin persoonsgegevens worden verwerkt (verzamelen, bewaren, gebruiken, verstrekken in brede zin). Proceseigenaren en uitvoerders zijn een belangrijke schakel in het voldoen aan privacybeleid, reglementen en wettelijke vereisten. Zij zijn immers degene die binnen de dagelijkse gang van zaken grip moeten houden op hun (deel)verantwoordelijkheid ten aanzien van privacy. De organisatie dient hen daarin adequaat te ondersteunen.

Uit Checklist IBP:

- De IBP-organisatie is ingericht (taken en rollen) waarbij verantwoordelijkheden en taken zijn belegd bij medewerkers.
- Er is een geheimhoudingsovereenkomst voor medewerkers niet in vaste dienst.
- Afspraken over passend onderwijs zijn gemaakt en bekend bij de betrokken medewerkers.
- Afspraken jeugdhulpverlening zijn gemaakt en bekend bij de betrokken medewerkers.
- Er zijn afspraken over de uitwisseling van leerlingdossiers en –gegevens met andere scholen.
- Zijn de relevante medewerkers op de hoogte van de regels over het omgaan met leerling dossiers.
- Afspraken leerplicht en verzuim zijn gemaakt en bekend bij de betrokken medewerkers.
- Security awareness training is gegeven aan alle medewerkers.
- Er wordt aandacht geschonken aan ict-bekwaamheid leraar
- Leerlingen zijn geïnformeerd over IBP op school.
- Er wordt aandacht geschonken aan mediawijsheid en digitale geletterdheid van leerlingen.
- De leerlingenraad wordt bij IBP betrokken.
- Privacyreglement is gecommuniceerd en opgenomen op website en/of in schoolgids.
- Sociale-mediareglement is bekend gemaakt aan alle betrokkenen.
- Gedragscode ict- en internetgebruik is bekend gemaakt aan alle betrokkenen.
- Ouders worden actief benaderd en geïnformeerd over IBP op school en gewezen op hun rechten.
- De (G)MR is (wordt regelmatig) geïnformeerd over IBP op school.

	VOLDOET NIET	VOLDOET BEPERKT	VOLDOET GROTENDEELS	VOLDOET GEHEEL	NIET VAN TOEPASSING
a.* Proceseigenaren en uitvoerders die verantwoording dragen voor de verwerking van persoonsgegevens hebben kennis van het privacybeleid en weten waaraan zij moeten voldoen.					

b.* Proceseigenaren en uitvoerders die verantwoording dragen voor de verwerking van persoonsgegevens handelen conform het privacybeleid en houden zich aan wet- en regelgeving.					
c.* Proceseigenaren en uitvoerders die verantwoording dragen voor de verwerking van persoonsgegevens zijn op de hoogte van welke persoonsgegevens zij wel en niet mogen verwerken.					
d. Proceseigenaren en uitvoerders rapporteren bij incidenten en periodiek over het behaalde privacybeschermingsniveau.					
e. De functieomschrijving van deze proceseigenaren en uitvoerders biedt de ruimte om de verantwoordelijkheid voor privacy gerelateerde kwesties binnen hun functie bij hen te beleggen.					
f. Deze proceseigenaren en uitvoerders hebben voldoende bevoegdheden en kennis om binnen hun verantwoordelijkheidsgebied zorg te dragen voor adequate uitvoering van het privacybeleid en het voldoen aan wet- en regelgeving.					
g. Deze proceseigenaren en uitvoerders hebben voldoende tijd en middelen om hun kennis ten aanzien van privacy gerelateerde zaken en situaties binnen hun verantwoordelijkheidsdomein actueel en toereikend te houden.					
h. Deze Proceseigenaren en uitvoerders worden adequaat begeleid bij hun taakstelling ten aanzien van de uitvoering van het privacybeleid en het voldoen aan wet- en regelgeving.					
i.* Deze Proceseigenaren en uitvoerders worden gehouden aan een geheimhoudingsplicht met betrekking tot het uitvoeren van hun taken.					
j.* Conclusie:					

2.2* Managers & Coördinatoren

2.3* Functionaris gegevensbescherming (FG)

2.4* Toezichthouders (compliance)

3. Externe partijen

De met een (*) gemarkeerde onderwerpen en aspecten zijn vereisten van de AVG.

Indien onderwerpen of aspecten naar uw inzicht niet van toepassing zijn voor uw organisatie, dan is het raadzaam in ieder geval te overwegen of en zo ja; hoe deze van invloed zijn op het privacybeschermingsniveau en het voldoen aan wet- en regelgeving.

3.1* Gegevensverantwoordelijken en Gegevensverwerkers (extern)

In relaties met of als gegevensverantwoordelijke en gegevensverwerker voldoet de organisatie aan wet- en regelgeving.

Toelichting

Om uitvoering te geven aan het privacybeleid en privacy adequaat te beschermen worden bij aanname of het uitbesteden van de verwerking van persoonsgegevens overeenkomsten afgesloten die voldoen aan wet- en regelgeving. De organisatie verzekert zich er binnen haar mogelijkheden van dat de organisaties waar persoonsgegevens worden verwerkt of die persoonsgegevens voor de organisatie verwerken een adequaat privacybeleid voeren en zich houden aan wet- en regelgeving. De AVG vereist hierin een proactieve rol van de organisatie. Indien de organisatie vaststelt of gerede twijfel heeft of de derde partij zich aan wet- en regelgeving houdt dan dient zij daar consequenties aan te verbinden. Deze kunnen bestaan uit het vereisen van passende maatregelen of afzien van samenwerking op het gebied van bewerking van persoonsgegevens.

Uit Checklist IBP:

- Er zijn afspraken gemaakt met leveranciers, die persoonsgegevens verwerken (beheer en toetsing contracten) Verwerkersovereenkomsten.
- De Privacy bijsluiter van de verwerkers-overeenkomsten zijn gepubliceerd.
- Afspraken over passend onderwijs zijn gemaakt en bekend bij de betrokken medewerkers.
- Afspraken jeugdhulpverlening zijn gemaakt en bekend bij de betrokken medewerkers.
- Er zijn afspraken over de uitwisseling van leerlingdossiers en –gegevens met andere scholen.

	VOLDOET NIET	VOLDOET BEPERKT	VOLDOET GROTENDEELS	VOLDOET GEHEEL	NIET VAN TOEPASSING
a.* Met derde partijen (verwerkingsverantwoordelijken) waarvoor bewerkingen worden uitgevoerd en waartoe de organisatie zich als verwerker verhoudt zijn bewerkingsovereenkomsten afgesloten die voldoen aan wet- en regelgeving.					
b.* Met derde partijen (bewerkers) die bewerkingen uitvoeren en waartoe de organisatie zich als verwerkingsverantwoordelijke verhoudt zijn bewerkingsovereenkomsten afgesloten die voldoen aan wet- en regelgeving.					

c.* Bij het uitwisselen van persoonsgegevens in de relatie verwerkingsverantwoordelijke en verwerker houdt de organisatie zich aan wet- en regelgeving waarin uitdrukkelijk doch niet uitsluitend wordt voldaan aan de beginselen van rechtmatigheid, behoorlijkheid, transparantie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en verantwoordingsplicht zoals de AVG dat vereist.					
d.* De organisatie - als verwerkingsverantwoordelijke - vereist aantoonbaar dat verwerkers en sub verwerkers voldoen aan wet en regelgeving en in het bijzonder de AVG.					
e.* De organisatie doet aantoonbaar navraag naar de aanwezigheid, uitvoering van en voldoen aan privacybeleid indien zij als verwerkingsverantwoordelijke of verwerker een relatie met een derde aangaat.					
f.* De organisatie ziet af van ontvangst of verstrekking van persoonsgegevens indien blijkt dat deze derde partij onvoldoende privacybestendig is.					
g.* De organisatie wisselt geen persoonsgegevens uit met derden indien op basis van feiten of omstandigheden ernstig getwijfeld moet worden aan de kwaliteit van het privacybeleid van die derden.					
h.* De organisatie voert bij een doorgifte van persoonsgegevens naar derde landen (landen buiten de EER) controle uit op het beschermingsniveau van persoonsgegevens bij het derde land.					
i.* Als de organisatie constateert dat het derde land niet beschikt over een passend beschermingsniveau, zorgt zij dat er is voldaan aan een van de overige voorwaarden voor doorgifte van persoonsgegevens naar dat derde land.					
j.* Conclusie:					

3.2* Ontvangers en verstrekkers van gegevens

4. Middelen

De met een (*) gemarkeerde onderwerpen en aspecten zijn vereisten van de AVG.
Indien onderwerpen of aspecten naar uw inzicht niet van toepassing zijn voor uw organisatie, dan is het raadzaam in ieder geval te overwegen of en zo ja; hoe deze van invloed zijn op het

privacybeschermingsniveau en het voldoen aan wet- en regelgeving.

4.1* Financieel

De organisatie zet ten behoeve van de effectieve uitvoering van het privacybeleid voldoende financiele middelen in.

Toelichting

Er dienen binnen de organisatie voldoende financiële middelen beschikbaar te zijn en – bij voorkeur planmatig /in de begrotingscyclus - worden toegewezen voor uitvoering van het privacybeleid. Degene die belast zijn met de coördinatie en ondersteuning van privacy gerelateerde zaken dienen structureel voldoende financiële middelen beschikbaar te hebben om hun taken effectief uit te voeren. Bij het vormgeven en beheren van processen dient functioneel, operationeel en financieel rekening te zijn gehouden met privacybescherming en de wettelijke vereisten (o.a. privacy by design & privacy by default). Ook voor het creëren van bewustzijn, draagvlak en kennis van privacy onder de uitvoerders van de werkprocessen zijn financiële middelen nodig . Verder vereist de AVG een adequate informatievoorziening over rechten van betrokkenen en ondersteuning bij het uitoefenen daarvan. Zowel de informatie en communicatie als technische en operationele invulling daarvan dienen structureel te zijn en vereisen financiële middelen.

	VOLDOET NIET	VOLDOET BEPERKT	VOLDOET GROTENDEELS	VOLDOET GEHEEL	NIET VAN TOEPASSING
a.* De organisatie stelt de voor adequate privacybescherming benodigde financiële middelen ter beschikking.					
b. De financiële middelen voor het inrichten en uitvoeren van privacymanagement in de organisatie zijn bekend, toereikend, beschikbaar en zijn of worden periodiek en/of planmatig toegewezen.					
c. De financiële middelen voor het privacybestendig maken van processen door proceseigenaren zijn bekend, toereikend, beschikbaar en zijn of worden periodiek en/of planmatig toegewezen.					
d. De financiële middelen voor implementatie, bewustwording, draagvlak en opleiding van medewerkers ten aanzien van privacybestendig werken zijn bekend, toereikend, beschikbaar en zijn of worden periodiek en/of planmatig toegewezen.					
e. De financiële middelen voor zowel technische als operationele realisatie van de vereiste informatievoorziening over rechten van betrokkenen en de ondersteuning bij het uitoefenen daarvan zijn bekend, toereikend, beschikbaar en zijn of worden periodiek en/of planmatig toegewezen.					
f. De financiële middelen voor effectief en onafhankelijk toezicht zijn bekend, toereikend, beschikbaar en zijn of worden periodiek en/of planmatig toegewezen.					
g.* Conclusie:					

4.2* Gebouwen en faciliteiten

5. Privacy aspecten binnen operationele processen & procedures

De met een (*) gemarkeerde onderwerpen en aspecten zijn vereisten van de AVG.

Indien onderwerpen of aspecten naar uw inzicht niet van toepassing zijn voor uw organisatie, dan is het raadzaam in ieder geval te overwegen of en zo ja; hoe deze van invloed zijn op het privacybeschermingsniveau en het voldoen aan wet- en regelgeving.

De AVG stelt uitgebreide eisen ten aanzien van de inrichting en documentatie van processen. Naast de privacy-specifieke processen die de AVG vereist, dienen de operationele werkprocessen waarin persoonsgegevens worden verwerkt privacybestendig te zijn. Daarnaast dienen afdelingen en processen als inkoop, informatiebeveiliging, ICT en compliance in hun ondersteunende taakstelling ook te zijn gericht op het optimaliseren van privacybescherming elders in de organisatie.

5.1* Beheersing van privacy in werkprocessen en verwerkingen

De werkprocessen en verwerkingen binnen de organisatie zijn privacybestendig.

Toelichting

Het realiseren en borgen van een privacybestendige organisatie vindt in de basis plaats door de werkprocessen, waar persoonsgegevens worden verwerkt (verzamelen, beheren, gebruiken, verstrekken, in brede zin), ook ten aanzien van het beschermen van privacy te optimaliseren. Een adequate inrichting van processen waarbij in de ontwerpfase al rekening is gehouden met privacyaspecten helpt de organisatie bij het voldoen aan wet- en regelgeving. Het brengt de organisatie en de verantwoordelijken doelmatiger 'in control' en minimaliseert inspanningen ten aanzien van privacymanagement, coördinatie- en toezicht.

Door uitvoering van de procesinventarisatie, het registreren van processen en bewerkingen in het bewerkingsregister – waarbij een korte basisanalyse op onderstaande punten plaatsvindt – en het eventueel uitvoeren van Proces-DPIA's aldaar, stelt u het onderstaande per werkproces vast.

Evaluatie op onderstaande punten betreft de samenvoeging van alle werkprocessen en heeft tot doel inzicht te verschaffen en eventueel geaggregeerd te verantwoorden op organisatieniveau. Deze onderliggende informatie per werkproces dient of is bedoeld beschikbaar te zijn in en via het verwerkingsregister.

Uit Checklist IBP:

- De medewerkers weten waar de IBP over gaat. Zij zijn bekend met de basisbegrippen, de aandachtspunten AVG en de 5 vuistregels.
- Afspraken over passend onderwijs zijn gemaakt en bekend bij de betrokken medewerkers.
- Afspraken jeugdhulpverlening zijn gemaakt en bekend bij de betrokken medewerkers.
- Er zijn afspraken over de uitwisseling van leerlingdossiers en –gegevens met andere scholen.
- Zijn de relevante medewerkers op de hoogte van de regels over het omgaan met leerling dossiers.
- Afspraken leerplicht en verzuim zijn gemaakt en bekend bij de betrokken medewerkers.
- Security awareness training is gegeven aan alle medewerkers.
- Er is een proces om autorisaties te controleren.
- Met Privacy by design, privacy by default wordt rekening gehouden.
- Er wordt aandacht geschonken aan ict-bekwaamheid leraar.
- Leerlingen zijn geïnformeerd over IBP op school.
- Er wordt aandacht geschonken aan mediawijsheid en digitale geletterdheid van leerlingen.
- De leerlingenraad wordt bij IBP betrokken.
- Privacyreglement is gecommuniceerd en opgenomen op website en/of in schoolgids.
- Sociale-mediareglement is bekend gemaakt aan alle betrokkenen.
- Gedragscode ict- en internetgebruik is bekend gemaakt aan alle betrokkenen.
- Ouders worden actief benaderd en geïnformeerd over IBP op school en gewezen op hun rechten.
- De (G)MR is (wordt regelmatig) geïnformeerd over IBP op school.

	VOLDOET NIET	VOLDOET BEPERKT	VOLDOET GROTENDEELS	VOLDOET GEHEEL	NIET VAN TOEPASSING
a.* Werkprocessen (waarin persoonsgegevens worden verwerkt) zijn beschreven.					
b.* Werkprocessen hebben een procesverantwoordelijke.					

c.* Binnen het werkproces zijn passende technische en organisatorische maatregelen getroffen om de privacy te waarborgen en aan wet- en regelgeving te voldoen.					
d.* Bij het ontwerp of herontwerp van werkprocessen wordt adequaat rekening gehouden met privacy aspecten en wordt, zoveel als redelijkerwijs in verhouding staat tot de schaal en de risico's van het proces voor betrokkenen, gericht op privacy by design en privacy by default.					
e. Er zijn indicatoren beschikbaar die het mogelijk maken de risico bestendigheid van het werkproces te beoordelen.					
f.* Binnen de werkprocessen worden persoonsgegevens verwerkt op een wijze die ten aanzien van de betrokkene (degene van wie de persoonsgegevens zijn) rechtmatig, behoorlijk en transparant is (rechtmatigheid, behoorlijkheid en transparantie).					
g.* De doeleinden van de verwerking in het werkproces zijn welbepaald, uitdrukkelijk omschreven en gerechtvaardigd en worden vervolgens niet op een daarmee onverenigbare wijze verwerkt (verzamelen, beheren, gebruiken, verstrekken, in brede zin) (doelbinding).					
h.* Binnen de werkprocessen worden niet meer persoonsgegevens verwerkt dan noodzakelijk voor het bereiken van het doel van de respectieve processen (minimale gegevensverwerking en doelbinding).					
i.* Binnen de werkprocessen worden alleen die persoonsgegevens verwerkt die noodzakelijk zijn voor het bereiken van het doel van de respectieve processen (minimale gegevensverwerking en doelbinding).					
j.* Binnen het werkproces zijn alle redelijke maatregelen genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren (juistheid).					
k.* De binnen het werkproces te verwerken of verwerkte persoonsgegevens worden bewaard in een vorm die er in voorziet dat betrokkenen niet langer te identificeren zijn dan voor de doeleinden van de bewerking noodzakelijk is (opslagbeperking).					

l.* De binnen de werkprocessen verwerkte persoonsgegevens worden niet langer beschikbaar gehouden dan voor het doel van het proces noodzakelijk is (opslagbeperking).					
m.* De binnen de werkprocessen te verwerken persoonsgegevens zijn beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (integriteit en vertrouwelijkheid).					
n.* De organisatie is verantwoordelijk voor naleving van de voornoemde punten / wettelijke vereisten en kan dit aantonen (verantwoordingsplicht).					
o. Conclusie:					

5.2* Inkoop

5.3* Informatiebeveiliging en -beleid

6. Privacy specifieke processen & procedures (AVG)

De met een (*) gemarkeerde onderwerpen en aspecten zijn vereisten van de AVG.

Indien onderwerpen of aspecten naar uw inzicht niet van toepassing zijn voor uw organisatie, dan is het raadzaam in ieder geval te overwegen of en zo ja; hoe deze van invloed zijn op het privacybeschermingsniveau en het voldoen aan wet- en regelgeving.

De AVG stelt uitgebreide eisen ten aanzien van de aanwezigheid, inrichting en documentatie van privacy specifieke processen. Gegevensverwerkingen dienen te zijn opgenomen in een bewerkingsregister; Analyseprocessen en beheerprocessen dienen vast te liggen (DPIA's) ; Waarborgende processen ten aanzien van transparantie naar en uitoefening van rechten door betrokkenen (degene van wie de persoonsgegevens zijn) dienen te zijn vastgesteld en gedocumenteerd.

6.1* Organisatie-DPIA (Data Protection Impact Assessment op organisatieniveau)

6.2* Proces DPIA's (Data Protection Impact Assessment op procesniveau)

De proces-DPIA's worden adequaat ingezet en ondersteunen de uitvoering van het privacybeleid effectief.

Toelichting

Wanneer een soort verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen (betrokkenen) dan vereist de AVG dat voorafgaand aan de verwerking een Proces-DPIA wordt uitgevoerd.

Een verhoogt risico kan bestaan door het gebruik van nieuwe technologieën, aard, context en doeleinden van de beoogde verwerking. Een Proces-DPIA is met name vereist voor verwerken die een of meer van onderstaande kenmerken in zich dragen:

- *Systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking , waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen.*
- *Grootschalige verwerking van bijzondere categorieën van persoonsgegevens (AVG; art 9, lid 1) of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten (AVG; Art. 10).*
- *Stelselmatige en grootschalige monitoring van openbare ruimten.*

In de submodule 'Kaarten' onder 'ontwikkelen' vindt u kant en klare formats voor het uitvoeren van Proces-DPIA's.

Uit Checklist IBP:

- IBP-verantwoordelijke en proces-eigenaren weten wat de achtergrond van de te realiseren maatregelen zijn.
- IBP-verantwoordelijke en proces-eigenaren hebben gegevens en processen geclassificeerd.
- IBP-verantwoordelijke en met proces-eigenaren hebben de huidige situatie in beeld gebracht en een Risicoanalyse gedaan.
- IBP-verantwoordelijke en proces-eigenaren hebben op basis van de risicoanalyse de belangrijkste te nemen maatregelen bepaald en vastgesteld.
- IBP-verantwoordelijke en proces-eigenaren hebben een planning gemaakt van de actiepunten (activiteitenplanning).
- IBP-verantwoordelijke en proces-eigenaren hebben verbetervoorstellen IBP in de planning opgenomen.
- Er is een standaard sjabloon gegevensbeschermingseffectbeoordeling aanwezig.
- Er is een overzicht van alle leveranciers/externen, die persoonsgegevens in opdracht van de organisatie verwerken.
- Afspraken rondom cameratoezicht zijn geregeld en gecommuniceerd.

	VOLDOET NIET	VOLDOET BEPERKT	VOLDOET GROTENDEELS	VOLDOET GEHEEL	NIET VAN TOEPASSING
a.* Proces-DPIA's worden voorafgaand aan de respectieve bewerking en bij aanpassing van die bewerking of verandering van het risico daarvan uitgevoerd.					
b.* Proces-DPIA's behandelen en beschrijven minimaal de onderdelen die volgens de AVG verplicht zijn.					
c.* Het uitvoeringsproces van Proces-DPIA's is systematisch en vastgelegd.					
d.* Voor het uitvoeren van een Proces-DPIA is een eindverantwoordelijke aangewezen.					
e.* De eindverantwoordelijke en uitvoerenden hebben voldoende informatie, bevoegdheden, rechten, plichten en bewegingsvrijheid om hun taken effectief en onafhankelijk te kunnen uitvoeren en daarover zonder aan de persoon gebonden risico te kunnen rapporteren.					
f.* Een Proces-DPIA geeft de proceseigenaar en de organisatie een adequaat beeld van het niveau van privacybescherming, privacyrisico's en in welke mate wordt voldaan aan wet en regelgeving.					
g.* Een Proces-DPIA geeft de organisatie een adequaat beeld op welke gebieden en aspecten, ten aanzien van het respectieve proces en/of de bewerkingen, maatregelen nodig zijn om aan de wettelijke vereisten en de bepalingen in het privacybeleid te voldoen.					
h.* Een Proces-DPIA geeft de organisatie een adequaat beeld van de ten behoeve van het respectieve proces te initiëren en reeds geïnitieerde verbeteracties en de status en deadlines daarvan.					
i.* Indien uit een Proces-DPIA blijkt dat de verwerking een hoog risico oplevert indien de verwerkingsverantwoordelijke geen maatregelen neemt, dan raadpleegt de organisatie de toezichthoudende autoriteit voorafgaand aan de verwerking.					
j.* Conclusie:					

6.3* Verwerkingsregistratie en verwerkingsregister

Het bewerkingsregister wordt adequaat ingezet en ondersteunt de uitvoering van het privacybeleid effectief.

Toelichting

De AVG stelt verplicht dat organisaties de bewerkingen (verzamelen, beheren, gebruiken, verstrekken, in brede zin) van persoonsgegevens vastleggen in het bewerkingsregister. Deze registraties moeten aan bepaalde eisen voldoen.

Indien uw organisatie minder dan 250 personen in dienst heeft is deze verplichting niet van toepassing.

TENZIJ:

- *De verwerking die wordt verricht waarschijnlijk een risico inhoud voor de rechten en vrijheden van betrokkenen.*
- *De verwerking **niet** incidenteel is (**opgelet**: Verwerkingen zijn zelden incidenteel. Het bijhouden van persoonsgegevens in de salarisadministratie, het bijhouden van relatiegegevens of versturen van nieuwsbrieven is bijvoorbeeld niet incidenteel).*
- *De verwerking betreft bijzondere categorieën van persoonsgegevens (AVG: Art 9, lid 1)*
- *De verwerking persoonsgegevens in verband met strafrechtelijke veroordelingen en strafbare feiten (AVG: Art. 10)*

Het voorgaande betekent in de praktijk dat vrijwel iedere organisatie een bewerkingsregister moet bijhouden.

Het bewerkingsregister bouwt en onderhoudt u eenvoudig en doelmatig in de submodule 'kaarten' onder 'ontwikkelen'. U doet daar direct een korte check en indien een proces-DPIA vereist blijkt, voegt u deze met een druk op de knop aan de bewerking toe.

Uit Checklist IBP:

- IBP-verantwoordelijke en proces-eigenaren weten wat de achtergrond van de te realiseren maatregelen zijn.
- IBP-verantwoordelijke en proces-eigenaren hebben gegevens en processen geclassificeerd.
- IBP-verantwoordelijke en met proces-eigenaren hebben de huidige situatie in beeld gebracht en een Risicoanalyse gedaan.
- IBP-verantwoordelijke en proces-eigenaren hebben op basis van de risicoanalyse de belangrijkste te nemen maatregelen bepaald en vastgesteld.
- IBP-verantwoordelijke en proces-eigenaren hebben een planning gemaakt van de actiepunten (activiteitenplanning).
- IBP-verantwoordelijke en proces-eigenaren hebben verbetervoorstellen IBP in de planning opgenomen.
- Er is een overzicht van alle leveranciers/externen, die persoonsgegevens in opdracht van de organisatie verwerken.
- Er is een overzicht van alle applicaties waarin persoonsgegevens verwerkt worden (intern).
- Afspraken rondom cameratoezicht zijn geregeld en gecommuniceerd.

	VOLDOET NIET	VOLDOET BEPERKT	VOLDOET GROTENDEELS	VOLDOET GEHEEL	NIET VAN TOEPASSING
a.* De organisatie beschikt over een register van alle verwerkingsactiviteiten					
b.* Het verwerkingsregister bevat alle verplichte informatie.					
c.* Het verwerkingsregister is actueel.					
d.* De organisatie beschikt over een procedure voor het actueel houden van het verwerkingsregister.					
e.* De organisatie heeft een eindverantwoordelijke voor het beheren en actualiseren van het bewerkingsregister aangewezen.					
f.* De eindverantwoordelijke heeft voldoende informatie, bevoegdheden, rechten, plichten, kwaliteiten en bewegingsvrijheid om zijn of haar taken effectief en onafhankelijk te kunnen uitvoeren en daarover zonder aan de persoon gebonden risico te kunnen rapporteren.					
g.* Conclusie:					

6.4* Datalekken (inbreuk privacy)

6.5* Documentatie & Verantwoording

7. Transparantie, informatievoorziening en rechten van betrokkenen

De met een (*) gemarkeerde onderwerpen en aspecten zijn vereisten van de AVG.

Indien onderwerpen of aspecten naar uw inzicht niet van toepassing zijn voor uw organisatie, dan is het raadzaam in ieder geval te overwegen of en zo ja; hoe deze van invloed zijn op het privacybeschermingsniveau en het voldoen aan wet- en regelgeving.

7.1* Informatievoorziening en informatieverzoeken met betrekking tot persoonsgegevens.

De informatievoorziening van de organisatie is effectief en voldoet aan wet- en regelgeving.

Toelichting

Uit Checklist IBP:

- Rechten betrokkenen zijn vastgelegd en gecommuniceerd naar medewerkers, leerlingen en ouders.
- Er is een procesbeschrijving hoe betrokkenen hun rechten kunnen uitoefenen
- Afspraken en procedures over privacy zijn geregeld en gecommuniceerd (informatieplicht, transparantie).
- De Privacy bijsluiter van de verwerkers-overeenkomsten zijn gepubliceerd

	VOLDOET NIET	VOLDOET BEPERKT	VOLDOET GROTENDEELS	VOLDOET GEHEEL	NIET VAN TOEPASSING
a.* De organisatie draagt er zorg voor en borgt dat informatie en communicatie, naar betrokkenen in verband met verwerkingen van persoonsgegevens in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal plaats vindt. Passend bij de doelgroep en met name indien het voor kinderen bestemd is.					
b.* De organisatie voorziet erin dat deze informatie schriftelijk of elektronisch beschikbaar wordt gemaakt en heeft een protocol en proces vastgesteld dat er in voorziet en borgt dat deze informatie, indien de betrokkende daarom verzoekt, ook mondeling kan worden / wordt meegedeeld op voorwaarde dat de identiteit van de betrokkene is bewezen.					
c.* De organisatie heeft een procedure en proces ingeregeld dat er in voorziet en borgt dat onverwijld, doch uiterlijk binnen een maand na ontvangst van het informatieverzoek met betrekking tot persoonsgegevens, informatie over het gevolg (opvolging of informatie zelf) aan betrokkene wordt verstrekt.					
d.* Voornoemde procedure voorziet erin dat, indien niet aan een informatieverzoek kan worden voldaan, de betrokkene onverwijld, doch uiterlijk binnen een maand na ontvangst, daarover en inclusief de redenen wordt geïnformeerd. De betrokkene wordt daarbij geïnformeerd over de mogelijkheid een klacht in te dienen bij de toezichthoudende autoriteit (AP) en beroep bij de rechter in te stellen.					
e. De organisatie heeft een eindverantwoordelijke voor dit proces aangewezen.					
f. De eindverantwoordelijke heeft voldoende informatie, bevoegdheden, rechten, plichten, kennis, kwaliteiten en bewegingsvrijheid om zijn of haar taken effectief en onafhankelijk te kunnen uitvoeren en daarover zonder aan de persoon gebonden risico te kunnen rapporteren.					
g.* De organisatie is bekend met de wettelijke beperkingen op deze bepaling en neemt deze hierbij in acht.					

h.* Bij inregelen van het proces is, zoveel als redelijkerwijs mogelijk en rekening houdend met de beschikbare technologie en de uitvoeringskosten, gericht op ‘privacy by design’ en ‘privacy by default’.					
i.* Conclusie:					

7.2* Informatievoorziening indien de persoonsgegevens bij de betrokkene worden verzameld (direct)

7.3* Informatievoorziening indien de persoonsgegevens niet van de betrokkene zijn verkregen (indirect)

7.4* Verkrijgen van toestemming en het recht op intrekken van toestemming

De organisatie zorgt dat, wanneer dat vereist is, toestemming van betrokkene wordt verkregen, toetst de rechtmatigheid daarvan en legt die toestemming, conform wet- en regelgeving vast. De organisatie zorgt dat de betrokkene zijn recht om toestemming in te trekken effectief en conform wet- en regelgeving kan uitoefenen.

Toelichting

(AVG: Art 7) *Voorwaarden voor toestemming*

Wanneer de verwerking berust op toestemming, moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens.

Indien de betrokkene toestemming geeft in het kader van een schriftelijke verklaring die ook op andere aangelegenheden betrekking heeft, wordt het verzoek om toestemming in een begrijpelijke, gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal gepresenteerd, zodanig dat een duidelijk onderscheid kan worden gemaakt met de andere aangelegenheden. Wanneer een gedeelte van een dergelijke verklaring een inbreuk vormt op deze verordening, is dit gedeelte niet bindend.

De betrokkene heeft het recht zijn toestemming te allen tijde in te trekken. Het intrekken van de toestemming doet geen afbreuk aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan. Voordat de betrokkene zijn toestemming geeft, wordt hij daarvan in kennis gesteld.

Het intrekken van de toestemming is even eenvoudig als het geven ervan.

Toestemming dient vrijelijk te zijn gegeven. Bij de beoordeling van de vraag of de toestemming vrijelijk kan worden gegeven, wordt onder meer ten sterkste rekening gehouden met de vraag of voor de uitvoering van een overeenkomst, met inbegrip van een dienstenovereenkomst, toestemming vereist (en/of gevraagd) is voor een verwerking van persoonsgegevens die niet noodzakelijk is voor de uitvoering van die overeenkomst.

(AVG Art. 8) *Voorwaarden voor de toestemming van kinderen met betrekking tot diensten van de informatiemaatschappij*

Wanneer uitdrukkelijke toestemming wordt verleent in verband met een rechtstreeks aanbod van diensten van de informatiemaatschappij aan een kind, is de verwerking van persoonsgegevens van een kind rechtmatig wanneer het kind ten minste 16 jaar is.

Wanneer het kind jonger is dan 16 jaar is zulke verwerking slechts rechtmatig indien en voor zover de toestemming of machtiging tot toestemming in dit verband wordt verleend door de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt.

Met inachtneming van de beschikbare technologie doet de verwerkingsverantwoordelijke redelijke inspanningen om in dergelijke gevallen te controleren of de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt, toestemming heeft gegeven of machtiging tot toestemming heeft verleend.

Het algemene overeenkomstenrecht (wetgeving), zoals de regels inzake de geldigheid, de totstandkoming of de gevolgen van overeenkomsten ten opzichte van kinderen, blijft van kracht.

Uit Checklist IBP:

- Rechten betrokkenen zijn vastgelegd en gecommuniceerd naar medewerkers, leerlingen en ouders.
- Er is een procesbeschrijving hoe betrokkenen hun rechten kunnen uitoefenen
- Afspraken en procedures over privacy zijn geregeld en gecommuniceerd (informatieplicht, transparantie).
- Toestemming ouders/leerlingen voor gebruik beeldmateriaal is geregeld.
- Procedure om toestemming in te trekken is vastgelegd en gecommuniceerd.
- Alle toestemmingen zijn aantoonbaar

	VOLDOET NIET	VOLDOET BEPERKT	VOLDOET GROTENDEELS	VOLDOET GEHEEL	NIET VAN TOEPASSING
a.* De organisatie beschikt over een protocol / procedure dat er in voorziet dat, wanneer vereist, toestemming wordt gevraagd, toestemming per betrokkene wordt vastgelegd en kan worden aangetoond, conform wet- en regelgeving.					
b.* De organisatie beschikt over een protocol / procedure die er in voorziet en borgt dat betrokkenen hun recht op het intrekken van toestemming zonder belemmering en onnodige vertraging, net zo eenvoudig als het geven van toestemming en conform wet- en regelgeving kunnen uitoefenen.					
c.* Het protocol / procedure voorziet er in dat de organisatie een redelijke inspanning doet om te achterhalen wat de leeftijd van de betrokkene is en daarbij de rechtmatigheid van de toestemming (met name m.b.t. kinderen) toetst.					
d. De organisatie heeft een eindverantwoordelijke voor dit proces aangewezen.					
e. De eindverantwoordelijke heeft voldoende informatie, bevoegdheden, rechten, plichten, kennis, kwaliteiten en bewegingsvrijheid om zijn of haar taken effectief en onafhankelijk te kunnen uitvoeren en daarover zonder aan de persoon gebonden risico te kunnen rapporteren.					
f.* De organisatie is bekend met de wettelijke beperkingen op deze bepaling en neemt deze in hierbij in acht.					
g.* Bij inregelen van het proces is, zoveel als redelijkerwijs mogelijk en rekening houdend met de beschikbare technologie en de uitvoeringskosten, gericht op ‘privacy by design’ en ‘privacy by default’.					
h.* Conclusie:					

7.5* Recht van inzage van de betrokkene

De organisatie zorgt dat de betrokkene zijn recht van inzage effectief en conform wet- en regelgeving kan uitoefenen.

Toelichting

Betrokkenen hebben het recht om van de verwerkingsverantwoordelijke uitsluitsel te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen.

Indien de betrokkene daartoe verzoekt dient de (verwerkingsverantwoordelijke) organisatie de betrokkene de bij wet- en regelgeving verplichte informatie te verstrekken. Indien de betrokkene om bijkomende kopieën verzoekt, kan de verwerkingsverantwoordelijke op basis van de administratieve kosten een redelijke vergoeding rekenen. Wanneer de betrokkene zijn verzoek elektronisch indient, en niet om een andere regeling verzoekt, wordt de informatie in een gangbare elektronische vorm verstrekt. Het verstrekken van kopieën doet geen afbreuk aan de rechten en vrijheden van anderen.

Persoonsgegevens waartoe een betrokkene het recht op inzage heeft:

1. *De verwerkingsdoeleinden;*
2. *De betrokken categorieën van persoonsgegevens;*
3. *Een overzicht van de persoonsgegevens die worden verwerkt.*
4. *De ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties;*
5. *Indien mogelijk, de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;*
6. *Dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken dat persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van hem betreffende persoonsgegevens wordt beperkt, alsmede het recht tegen die verwerking bezwaar te maken;*
7. *Dat de betrokkene het recht heeft een klacht in te dienen bij een toezichthoudende autoriteit;*
8. *Wanneer de persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens;*
9. *Het bestaan van geautomatiseerde besluitvorming, en of er sprake is van profilering en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.*
10. *Wanneer persoonsgegevens worden doorgegeven aan een derde land of een internationale organisatie, heeft de betrokkene het recht in kennis te worden gesteld van de passende waarborgen inzake de doorgifte.*

Uit Checklist IBP:

- Rechten betrokkenen zijn vastgelegd en gecommuniceerd naar medewerkers, leerlingen en ouders.
- Er is een procesbeschrijving hoe betrokkenen hun rechten kunnen uitoefenen
- Afspraken en procedures over privacy zijn geregeld en gecommuniceerd (informatieplicht, transparantie).

	VOLDOET NIET	VOLDOET BEPERKT	VOLDOET GROTENDEELS	VOLDOET GEHEEL	NIET VAN TOEPASSING
a.* De organisatie beschikt over een protocol / procedure die er in voorziet en borgt dat betrokkenen hun recht van inzage zonder belemmering en onnodige vertraging en conform wet- en regelgeving kunnen uitoefenen.					
b. De organisatie heeft een eindverantwoordelijke voor dit proces aangewezen.					
c. De eindverantwoordelijke heeft voldoende informatie, bevoegdheden, rechten, plichten, kennis, kwaliteiten en bewegingsvrijheid om zijn of haar taken effectief en onafhankelijk te kunnen uitvoeren en daarover zonder aan de persoon gebonden risico te kunnen rapporteren.					
d.* De organisatie is bekend met de wettelijke beperkingen op deze bepaling en neemt deze hierbij in acht.					
e.* Wanneer de betrokkene zijn verzoek tot inzage elektronisch indient, en niet om een andere regeling verzoekt, verstrekt de organisatie de informatie in een gangbare elektronische vorm.					
f.* Bij inregelen van het proces is, zoveel als redelijkerwijs mogelijk en rekening houdend met de beschikbare technologie en de uitvoeringskosten, gericht op ‘privacy by design’ en ‘privacy by default’.					
g.* Conclusie:					

7.6* Recht op rectificatie

De organisatie zorgt dat de betrokkene zijn recht op rectificatie effectief en conform wet- en regelgeving kan uitoefenen.

Toelichting

De betrokkene heeft het recht om van de verwerkingsverantwoordelijke direct of zonder onredelijke vertraging rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen. De betrokkene heeft er recht op dat onvolledige persoonsgegevens worden aangevuld zodat deze volledig zijn, doch niet meer dan voor de doeleinden van de verwerking noodzakelijk is. De betrokkene na daartoe onder meer een aanvullende verklaring verstrekken.

Uit Checklist IBP:

- Rechten betrokkenen zijn vastgelegd en gecommuniceerd naar medewerkers, leerlingen en ouders.
- Er is een procesbeschrijving hoe betrokkenen hun rechten kunnen uitoefenen
- Afspraken en procedures over privacy zijn geregeld en gecommuniceerd (informatieplicht, transparantie).

	VOLDOET NIET	VOLDOET BEPERKT	VOLDOET GROTENDEELS	VOLDOET GEHEEL	NIET VAN TOEPASSING
a.* De organisatie beschikt over een protocol / procedure die er in voorziet en borgt dat betrokkenen hun recht op rectificatie zonder belemmering en onnodige vertraging en conform wet- en regelgeving kunnen uitoefenen.					
b. De organisatie heeft een eindverantwoordelijke voor dit proces aangewezen.					
c. De eindverantwoordelijke heeft voldoende informatie, bevoegdheden, rechten, plichten, kennis, kwaliteiten en bewegingsvrijheid om zijn of haar taken effectief en onafhankelijk te kunnen uitvoeren en daarover zonder aan de persoon gebonden risico te kunnen rapporteren.					
d.* De organisatie rectificeert onjuiste persoonsgegevens direct of zo snel als redelijkerwijs mogelijk is.					
e.* De organisatie vult onvolledige persoonsgegevens aan voor zover passend bij de doeleinden van de verwerking en, indien daartoe een aanvullende verklaring benodigd is, na de ontvangst en eventuele verificatie van die verklaring.					
f.* De organisatie stelt iedere ontvanger aan wie persoonsgegevens zijn verstrekt, in kennis van elke rectificatie van persoonsgegevens, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. De verwerkingsverantwoordelijke verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.					
g.* De organisatie is bekend met de wettelijke beperkingen op deze bepaling en neemt deze hierbij in acht.					
h.* Bij inregelen van het proces is, zoveel als redelijkerwijs mogelijk en rekening houdend met de beschikbare technologie en de uitvoeringskosten, gericht op ‘privacy by design’ en ‘privacy by default’.					
i.* Conclusie:					

7.7* Recht op gegevenswissing (“recht op vergetelheid”)

7.8* Recht op beperking van de verwerking

7.9* Recht op overdraagbaarheid van gegevens (dataportabiliteit)

7.10* Recht op bezwaar en weigering geautomatiseerde besluitvorming (o.a. profilering)

V. Status (concluderend)

Status (concluderend)

Beoordeel aan de hand van uw vaststellingen of en zo ja; in welke mate, de organisatie in control en privacybestendig is en of daarbij aan wet- en regelgeving (AVG) wordt voldaan.

VI. Scholen en de AVG (AP)

Met de komst van de Algemene verordening gegevensbescherming (AVG) krijgt u als school meer verantwoordelijkheden om de persoonsgegevens van uw leerlingen goed te beschermen.

Digitalisering

Innovatieve, digitale systemen bieden interessante mogelijkheden om de kwaliteit van het onderwijs en de interne werkprocessen te verbeteren. Bijvoorbeeld met digitale toetsingsprogramma's, leerlingvolgsystemen en het gebruik van sociale media & apps. Maar deze nieuwe mogelijkheden om persoonsgegevens te verwerken, brengen ook de verantwoordelijkheid met zich mee om dat zorgvuldig en veilig te doen.

Onder de AVG moet u vooraf goed nadenken over de systemen waarmee u werkt of wilt gaan werken en hoe u die inricht (privacy by design). De standaardinstellingen moeten bovendien privacyvriendelijk zijn (privacy by default).

Verantwoordingsplicht

Nieuw onder de AVG is ook de verantwoordingsplicht. De verantwoordingsplicht houdt onder meer in dat u aan moet kunnen tonen welke technische en organisatorische maatregelen u hebt genomen om de persoonsgegevens van uw leerlingen te beschermen.

U moet aan de toezichthouder goed kunnen onderbouwen waarom u het recht hebt om bepaalde persoonsgegevens te verwerken. In sommige gevallen heeft u bijvoorbeeld toestemming nodig van leerlingen of hun ouders om persoonsgegevens te verwerken. Zoals voor het publiceren van foto's op uw website waarop leerlingen herkenbaar in beeld zijn. U moet dan kunnen laten zien dat u die toestemming heeft.

Overige regels

Onderstaand vindt u een aantal belangrijke onderwerpen en regels waar u specifiek als school rekening mee moet houden. Daarnaast gelden vanaf 25 mei 2018 natuurlijk ook de andere verplichtingen uit de AVG.

Data Protection Impact Assessment (DPIA)

Wanneer moeten scholen een DPIA uitvoeren?

Onder de Algemene verordening gegevensbescherming (AVG) kunnen organisaties verplicht zijn om een data protection impact assessment (DPIA) uit te voeren. Dat geldt ook voor scholen. Een DPIA is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert. Bijvoorbeeld voor de leerlingen van wie u persoonsgegevens verwerkt.

Wat is een DPIA?

Met een DPIA brengt u de privacyrisico's van een gegevensverwerking in kaart. Vervolgens kunt u maatregelen treffen om deze risico's te verkleinen.

Privacyrisico zelf beoordelen

Of een verwerking een hoog privacyrisico oplevert, moet u zelf beoordelen. De Europese privacytoezichthouders hebben 9 criteria voor een DPIA opgesteld die u helpen om dat te toetsen.

Meestal is een DPIA verplicht als uw verwerking voldoet aan 2 of meer van de 9 criteria.

De 9 criteria zijn:

1. beoordelen van mensen op basis van persoonskenmerken;
2. geautomatiseerde beslissingen;
3. stelselmatige en grootschalige monitoring;
4. gevoelige gegevens;
5. grootschalige gegevensverwerkingen;
6. gekoppelde databases;
7. gegevens over kwetsbare personen (bijvoorbeeld kinderen);
8. gebruik van nieuwe technologieën;
9. blokkering van een recht, dienst of contract.

Let op: deze 9 criteria zijn een handreiking om in te schatten of u een DPIA moet uitvoeren. Ook als u aan slechts één - of geen - van deze criteria voldoet, moet u goed kunnen onderbouwen waarom u ervoor kiest om geen DPIA uit te voeren. Dit maakt onderdeel uit van de verantwoordingsplicht die u onder de AVG heeft.

DPIA voor leerlingvolgsysteem en cameratoezicht

Gaat uw school gebruikmaken van een leerlingvolgsysteem of van cameratoezicht? Dan moet u voor deze verwerkingen waarschijnlijk een DPIA uitvoeren.

Voor bestaande verwerkingen geldt dat u alleen verplicht bent een DPIA uit te voeren als er iets verandert aan het risico van de gegevensverwerking. En de gegevensverwerking vervolgens (na de verandering) een hoog privacyrisico oplevert.

Leerlinggegevens

Waar moet u op letten als een andere organisatie leerlinggegevens namens uw school verwerkt?

Verwerkt een andere organisatie namens uw school leerlinggegevens? Bijvoorbeeld omdat u gebruik maakt van een bepaalde app of een online platform? Dan blijft u ook onder de Algemene verordening gegevensbescherming (AVG) verplicht om een overeenkomst op te stellen met de aanbieder. Onder de AVG heet dit een verwerkersovereenkomst.

Eisen verwerkersovereenkomst onder de AVG

In een verwerkersovereenkomst legt u de voorwaarden voor de gegevensverwerking vast. Nieuw is dat de AVG meer en gedetailleerdere eisen stelt aan dit soort overeenkomsten.

Bijvoorbeeld: stopt de samenwerking met de derde partij? Dan kunt u als school aangeven welke persoonsgegevens de verwerker na afloop van de verwerkingsdienst moet wissen of aan uw school terugbezorgen. De verwerker moet aan uw verzoek voldoen. Ook moet de verwerker bestaande kopieën verwijderen, tenzij de opslag verplicht is.

Verwerkingsregister

Wat moet een school in het register van verwerkingsactiviteiten opnemen?

Onder de Algemene verordening gegevensbescherming (AVG) zijn organisaties vaak verplicht om een register van verwerkingsactiviteiten op te stellen. Dat geldt ook voor scholen. In het register staat informatie over de persoonsgegevens die u verwerkt.

In de AVG staat welke informatie organisaties minimaal in het register van verwerkingsactiviteiten moeten opnemen. Voor het register van uw school betekent dat dat in ieder geval de volgende informatie in het register moet staan:

- de naam en contactgegevens van:

- uw organisatie, of de vertegenwoordiger van uw organisatie;
- eventuele andere organisaties met wie u gezamenlijk de doelen en middelen van de verwerking heeft vastgesteld;
- de functionaris voor de gegevensbescherming (FG) als u die heeft aangesteld;
- eventuele andere internationale organisaties waar u persoonsgegevens mee deelt.

- de doelen waarvoor u de persoonsgegevens verwerkt;
- een beschrijving van de categorieën van personen van wie u gegevens verwerkt. Denk hierbij onder meer aan ouders, voogden, leerlingen, docenten, begeleiders;
- een beschrijving van de categorieën van persoonsgegevens. Denk hierbij aan onder meer administratiegegevens van leerlingen, verzuimgegevens, gegevens over vorderingen en resultaten van leerlingen, handelingsplannen;
- de datum waarop u de gegevens moet wissen als dat bekend is;
- de categorieën van ontvangers aan wie u persoonsgegevens verstrekt. Denk hierbij onder meer aan externe instanties;
- deelt u de gegevens met een land of internationale organisatie buiten de EU? Dan moet u dit aangeven in het register;
- een algemene beschrijving van de technische en organisatorische maatregelen die u heeft genomen om persoonsgegevens die u verwerkt te beveiligen.

Verantwoordingsplicht

Als de Autoriteit Persoonsgegevens (AP) daar om vraagt, moet u het register van verwerkingsactivtiteiten kunnen laten zien. Dit maakt onderdeel uit van uw verantwoordingsplicht. Dit maakt onderdeel uit van de verantwoordingsplicht.

Leerlingvolgsystemen

Leerlingdossiers

Digitale onderwijstools

Digitale onderwijstools

Informeren over verwerking persoonsgegevens

Wanneer moet u leerlingen en ouders informeren over de persoonsgegevens die u verwerkt?

Net als onder de huidige Wet bescherming persoonsgegevens (Wbp) geldt onder de Algemene verordening gegevensbescherming (AVG) de informatieplicht. Voor u als school betekent dat dat u verplicht bent om leerlingen en ouders te informeren over het verwerken van persoonsgegevens. Zodat zij weten welke gegevens u over hen verzamelt en wat u er mee doet.

Wanneer het gaat om kinderen onder de 16 jaar, dan moet u de ouders om toestemming vragen. Gaat het leerlingen ouder dan 16 jaar? Dan moet u de leerlingen zelf om toestemming vragen.

Direct en indirect verzamelen

U moet ouders en leerlingen informeren over de persoonsgegevens die u:

- direct via de ouderen en/of leerlingen ontvangt; of
- indirect, via andere kanalen verzamelt. Bijvoorbeeld via andere personen of via openbare informatie op internet.

Wanneer hoeft u ouders en leerlingen niet te informeren?

Als u de informatie direct bij ouders en leerlingen verzamelt dan hoeft u hen niet te informeren als:

- de betrokken persoon al over de informatie beschikt;
- het informeren onmogelijk blijkt of onevenredig veel inspanning zou vergen;
- het verkrijgen of verstrekken van deze gegevens uitdrukkelijk is voorgeschreven bij unie of lidstatelijk recht;
- de persoonsgegevens vertrouwelijk moeten blijven vanwege beroepsgeheim of statutaire geheimhoudingsplicht.

Welke informatie moet u leerlingen en/of ouders geven over de persoonsgegevens die u verwerkt?

Waar moet u als school op letten als u ouders/leerlingen informeert over de gegevens die u verwerkt?

Toestemming beeldmateriaal

Hoe vraagt u onder de AVG toestemming voor het publiceren van beeldmateriaal van leerlingen?

Net als onder de huidige Wet bescherming persoonsgegevens (Wbp,) heeft u ook onder de Algemene verordening gegevensbescherming (AVG) toestemming nodig voor het publiceren van beeldmateriaal van leerlingen. Nieuw onder de AVG is dat u als school moet kunnen aantonen dat u toestemming heeft van de leerlingen of hun ouders/voogd.

Toestemming van leerling of ouder

Wilt u beeldmateriaal publiceren van een leerling van 16 jaar of ouder? Bijvoorbeeld online of in een papieren schoolkrant? Dan moet de leerling daarvoor zelf toestemming geven. Is de leerling jonger dan 16 jaar? Dan heeft u toestemming nodig van zijn of haar ouder. Het moet voor leerlingen en ouders net zo makkelijk zijn om de toestemming weer in te trekken als om de toestemming te geven.

Waar moet de toestemming aan voldoen?

Bij geldige toestemming moet elke twijfel zijn uitgesloten. De toestemming moet aan drie voorwaarden voldoen:

- de toestemming moet vrij en niet onder druk gegeven zijn. De leerling of ouder mag bijvoorbeeld niet benadeeld worden als hij of zij geen toestemming geeft.
- de toestemming moet ondubbelzinnig zijn. Het moet dus volstrekt helder zijn dát er toestemming is verleend. U mag niet uit gaan van het principe 'wie zwijgt, stemt toe'.
- u hebt toestemming gevraagd voor een specifieke verwerking en een specifiek doel. Bijvoorbeeld om via foto's en video's op uw website verslag te doen van een schoolreisje aan alle ouders.

Tip: u kunt ervoor kiezen om in een keer toestemming te vragen voor de publicatie van beeldmateriaal voor meerdere activiteiten gedurende het schooljaar. Maar let op: dit mag alleen als per activiteit aan bovenstaande drie voorwaarden is voldaan.

Mag u als school onder de AVG beeldmateriaal van leerlingen publiceren?

Ja, maar er gelden wel regels. Net als onder de huidige Wet bescherming persoonsgegevens (Wbp,) heeft u onder de Algemene verordening gegevensbescherming (AVG) toestemming nodig voor het publiceren van beeldmateriaal van leerlingen. Daarnaast moet u het beeldmateriaal goed beveiligen.

Nieuw onder de AVG is bijvoorbeeld dat u als school moet kunnen aantonen dat u toestemming heeft. En dat u maatregelen hebt genomen om het beeldmateriaal te beschermen.

Toestemming

Foto's en video's waarbij personen herkenbaar in beeld zijn, zijn persoonsgegevens. Wilt u beeldmateriaal publiceren van een leerling van 16 jaar of ouder? Dan moet de leerling daarvoor zelf toestemming geven. Is de leerling jonger dan 16 jaar? Dan heeft u toestemming nodig van zijn of haar ouder.

Onder de AVG moet u straks aan kunnen tonen dat u geldige toestemming van leerlingen en/of hun ouders hebt voor de publicatie van het beeldmateriaal. En het moet voor leerlingen en ouders net zo makkelijk zijn om de toestemming weer in te trekken als om de toestemming te geven.

Beveiligen

Vanuit zowel de Wbp als de AVG moet u als school extra maatregelen treffen om de privacy van leerlingen te beschermen. Het is belangrijk dat u de beelden beveiligt tegen misbruik. Onder de AVG moet u straks aan kunnen tonen dat u voldoende technische en organisatorische maatregelen hebt genomen om het beeldmateriaal van uw leerlingen te beschermen.

Ter illustratie: wilt u alleen ouders en leerlingen toegang geven tot beeldmateriaal? Dan kan het een passende maatregel zijn om een portal op uw website te plaatsen waar alleen leerlingen en ouders op in kunnen loggen. Die portal moet dan wel met https beveiligd zijn.

U kunt ook kiezen voor een app of andere online dienst waarmee u bepaalt wie u toegang wilt geven. Let bij het gebruik van (gratis) online diensten wel goed op wat de aanbieder met de persoonsgegevens doet. Lees altijd de privacy policy.

Overige regels

Het vragen van toestemming en het beveiligen van het beeldmateriaal, zijn twee belangrijke regels waar u als school rekening mee moet houden. Daarnaast gelden natuurlijk ook de andere verplichtingen uit de Wbp en vanaf 25 mei 2018 de AVG.

VII. Praktische vragen & uitleg (AP)

Bron: Autoriteit Persoonsgegevens 2018.

De hier aangeboden praktische uitleg is bedoeld behulpzaam te zijn. De verschillende onderwerpen uit de AVG die direct voor u van belang zijn worden handzaam en begrijpelijk uitgelegd. De beschrijvingen zijn handvatten en kunnen niet worden opgevat als wettelijke bepalingen. Wettelijke bepalingen vindt u verderop.

Voorbereiden: 10 onderwerpen en stappen

De onderstaande 10 onderwerpen en stappen geven u een globaal beeld van waar de introductie van de AVG voor u om zal gaan.

1. Bewustwording

Zorg ervoor dat de relevante mensen in uw organisatie (zoals beleidsmakers) op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op uw huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen. Houd er rekening mee dat de implementatie van de AVG veel kan vragen van de beschikbare menskracht en middelen en begin er daarom op tijd mee.

Bedenk dat de AP uw organisatie sancties kan opleggen van maximaal 20 miljoen euro of 4% van uw wereldwijde omzet als u zich niet aan de nieuwe privacywetgeving houdt.

2. Rechten van betrokkenen

Onder de AVG krijgen betrokkenen (de mensen van wie u persoonsgegevens verwerkt) meer en verbeterde privacyrechten. Zorg er daarom voor dat zij hun privacyrechten goed kunnen uitoefenen.

Denk daarbij aan bestaande rechten, zoals het recht op inzage en het recht op correctie en verwijdering. Maar houd ook alvast rekening met nieuwe rechten, zoals het recht op dataportabiliteit. Bij dit recht moet u ervoor zorgen dat betrokkenen hun gegevens makkelijk kunnen krijgen en vervolgens kunnen doorgeven aan een andere organisatie als ze dat willen.

Personen kunnen bij de AP klachten indienen over de manier waarop u met hun gegevens omgaat. De AP is verplicht deze klachten te behandelen.

3. Overzicht verwerkingen

Breng uw gegevensverwerkingen in kaart. Documenteer welke persoonsgegevens u verwerkt en met welk doel u dit doet, waar deze gegevens vandaan komen en met wie u ze deelt.

Onder de AVG heeft u een verantwoordingsplicht, wat inhoudt dat u moet kunnen aantonen dat uw organisatie in overeenstemming met de AVG handelt. Het bijhouden van een register van verwerkingsactiviteiten is onderdeel van de verantwoordingsplicht.

U kunt het register ook nodig hebben als betrokkenen hun privacyrechten uitoefenen. Als zij u vragen hun gegevens te corrigeren of verwijderen, moet u dit doorgeven aan de organisaties waarmee u hun gegevens heeft gedeeld.

4. Data protection impact assessment (DPIA)

Onder de AVG kunt u verplicht zijn een zogeheten data protection impact assessment (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico’s van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico’s te verkleinen.

U moet een DPIA uitvoeren als uw beoogde gegevensverwerking waarschijnlijk een hoog privacyrisico met zich meebrengt. U kunt nu alvast inschatten of u straks DPIA's moet uitvoeren en hoe u dit dan gaat aanpakken.

Komt straks uit een DPIA naar voren dat uw beoogde verwerking een hoog risico oplevert? En lukt het u niet om maatregelen te vinden om dit risico te beperken? Dan moet u met de AP overleggen voordat u met de verwerking start.

Dit wordt een voorafgaande raadpleging genoemd. De AP beoordeelt dan of de voorgenomen verwerking in strijd is met de AVG. Is dit het geval, dan ontvangt u een schriftelijk advies van de AP.

5. Privacy by design & privacy by default

Maak uw organisatie nu al vertrouwd met de onder de AVG verplichte uitgangspunten van privacy by design en privacy by default en ga na hoe u deze beginselen binnen uw organisatie kunt invoeren.

Privacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd. Maar bijvoorbeeld ook dat u niet meer gegevens verzameld dan noodzakelijk voor het doel van de verwerking. En dat u de gegevens niet langer bewaart dan nodig.

Privacy by default houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken. Bijvoorbeeld door:

- een app die u aanbiedt niet de locatie van gebruikers te laten registeren als dat niet nodig is;
- op uw website het vakje 'Ja, ik wil aanbiedingen ontvangen' niet vooraf aan te vinken;
- als iemand zich op uw nieuwsbrief wil abonneren niet meer gegevens te vragen dan nodig is.

6. Functionaris voor de gegevensbescherming

Onder de AVG kunnen organisaties verplicht zijn om een functionaris voor de gegevensverwerking (FG) aan te stellen. Bepaal nu alvast of dit voor uw organisatie geldt. Zo ja, wacht dan niet te lang met het werven van een FG. Uiteraard mag uw organisatie ook vrijwillig een FG aanstellen.

7. Meldplicht datalekken

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan uw eigen registratie van de datalekken die zich in uw organisatie hebben voorgedaan. U moet alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan.

Dit gaat verder dan de huidige protocolplicht uit de Wet bescherming persoonsgegevens, die alleen betrekking heeft op de gemelde datalekken.

De Europese privacytoezichthouders hebben in oktober 2017 guidelines gepubliceerd over de meldplicht datalekken onder de AVG. Deze guidelines zijn nog niet definitief, maar staan open voor publieke consultatie. Wanneer de guidelines definitief zijn, kunnen wij u volledig informeren over de meldplicht datalekken onder de AVG.

8. Verwerkersovereenkomsten

Heeft u uw gegevensverwerking uitbesteed aan een verwerker? (nu nog 'bewerker' genoemd)? Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met uw bewerkers nog steeds toereikend zijn. En of deze voldoen aan de eisen die de AVG aan verwerkersovereenkomsten stelt. Zo niet, breng dan tijdig noodzakelijke wijzigingen aan.

9. Leidende toezichthouder

Heeft uw organisatie vestigingen in meerdere EU-lidstaten? Of hebben uw gegevensverwerkingen in meerdere lidstaten impact? Dan hoeft u onder de AVG nog maar met één privacytoezichthouder zaken te doen. Dit wordt de leidende toezichthouder genoemd. Geldt dit voor uw organisatie, bepaal dan onder welke privacytoezichthouder u valt.

10. Toestemming

Uw gegevensverwerking kan gebaseerd zijn op toestemming van de betrokkenen. De AVG stelt strengere eisen aan toestemming. Evalueer daarom de manier waarop u toestemming vraagt, krijgt en registreert. Pas deze wijze indien nodig aan.

Nieuw is dat u moet kunnen aantonen dat u geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven.

Wanneer mag u persoonsgegevens verwerken

Wat wordt verstaan onder verwerken?

Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van
persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen,
structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van
doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of
vernietigen van gegevens.

De grondslagen: heeft u het recht om persoonsgegevens te verwerken?

U mag alleen '**gewone**' persoonsgegevens verwerken wanneer u aan ten minste 1 van de 6 AVG-grondslagen voldoet.

1. Toestemming
2. Noodzakelijk voor de uitvoering van een overeenkomst
3. Noodzakelijk voor het nakomen van een wettelijke verplichting
4. Noodzakelijk ter bescherming van vitale belangen
5. Noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag
6. Noodzakelijk voor de behartiging van de gerechtvaardigde belangen

De verwerking van bijzondere en strafrechtelijke persoonsgegevens is verboden. Tenzij u zich kunt beroepen op een specifieke wettelijke uitzondering én één van de grondslagen voor het verwerken van 'gewone' persoonsgegevens.

Wanneer u zich op welke van de grondslagen voor het verwerken van 'gewone' persoonsgegevens kunt beroepen leest u in de volgende paragrafen.

1. Grondslag: Toestemming

Bijvoorbeeld: u vraagt gebruikers van uw foto-app toestemming om locatiegegevens te verzamelen.

Locatiegegevens zijn persoonsgegevens. Eén van de voorwaarden voor rechtsgeldige toestemming voor gegevensverwerking is dat mensen de vrije keuze moeten hebben om toestemming te geven.

In dit voorbeeld moet iemand een foto-app dus ook kunnen gebruiken zonder deze toestemming te geven. Het verzamelen van locatiegegevens is immers niet direct noodzakelijk voor het maken en bewerken van foto's.

Wanneer mag u zich baseren op de grondslag toestemming?

U heeft alleen het recht om (gewone) persoonsgegevens te verwerken als u zich kunt baseren op 1 van de 6 grondslagen uit de AVG. Eén van die grondslagen is 'toestemming'. De AVG schrijft niet precies voor in welke vorm u toestemming moet vragen. Maar de manier waarop u toestemming vraagt moet wel voldoen aan een aantal specifieke eisen.

Rechstgeldige toestemming voldoet aan de volgende eisen:

- Vrijelijk gegeven: u mag iemand niet onder druk zetten om toestemming te geven. Bijvoorbeeld door iemand te benadelen als hij of zij geen toestemming geeft. Let daarbij op machtsverhoudingen: een werknemer kan een vraag van zijn werkgever bijvoorbeeld moeilijk weigeren.
- Ondubbelzinnig: er moet sprake zijn van een duidelijke actieve handeling. Bijvoorbeeld een (digitale) schriftelijke of een mondelinge verklaring. Het moet in elk geval volstrekt helder zijn dát er toestemming is verleend. U mag niet uit gaan van het principe 'wie zwijgt, stemt toe'. Het gebruik van voor-aangevinkte vakjes is dus niet toegestaan.
- Geïnformeerd: u moet mensen informeren over:
    - de identiteit van u als organisatie;
    - het doel van elke verwerking waarvoor u toestemming vraagt;
    - welke persoonsgegevens u verzamelt en gebruikt;
    - het recht dat zij hebben om de toestemming weer in te trekken. U moet de informatie in een toegankelijke vorm aanbieden. Ook moet deze begrijpelijk zijn zodat iemand een weloverwogen keuze kan maken. Dat betekent dat u duidelijke en eenvoudige taal moet gebruiken.
    - Specifiek: toestemming moet steeds gelden voor een specifieke verwerking en een specifiek doel. Indien u als organisatie bij de verwerking meerdere doeleinden heeft, dient u de betrokkene hierover te informeren en betrokkene voor elk doel afzonderlijk toestemming te vragen. Het doel mag niet gaandeweg veranderen.
    - Het moet voor mensen net zo makkelijk zijn om de toestemming weer in te trekken als dat het was om de toestemming te geven.
    - U moet kunnen aantonen dat u geldige toestemming heeft verkregen.

Voldoet de toestemming niet aan deze eisen? Dan is de toestemming niet geldig. U mag de persoonsgegevens dan niet verwerken.

Toestemming bij kinderen

De AVG geeft kinderen jonger dan 16 jaar extra bescherming. Want kinderen kunnen de risico's van een gegevensverwerking niet of minder goed inschatten. Daarom moeten zij toestemming hebben van de persoon die de ouderlijke verantwoordelijkheid draagt.

Verantwoordingsplicht

Wilt u zich baseren op de grondslag toestemming? Zorg er dan voor dat u kunt aantonen dat u die toestemming op de juiste manier heeft gevraagd en gekregen. Onder de AVG heeft u namelijk een verantwoordingsplicht.

2. Grondslag: Noodzakelijk voor de uitvoering van een overeenkomst

Bijvoorbeeld: u heeft de adresgegevens van klanten nodig om de bestelde producten bij hen thuis te bezorgen. Deze gegevens zijn noodzakelijk om de overeenkomst met uw klanten na te kunnen komen.

Zorg ervoor dat u goed kunt onderbouwen dat u zich op deze grondslag mag baseren. Zijn de persoonsgegevens echt noodzakelijk voor de naleving van de overeenkomst met ieder betrokken individu?

Wanneer mag u zich baseren op de grondslag uitvoering overeenkomst?

U heeft alleen het recht om persoonsgegevens te verwerken als u zich kunt baseren op minimaal 1 van de 6 AVG-grondslagen. Eén van die grondslagen is 'noodzakelijk voor de uitvoering van een overeenkomst'.

U mag zich op deze grondslag baseren als u een overeenkomst heeft met iemand en hiervoor het verwerken van persoonsgegevens noodzakelijk is. De overeenkomst zelf mag niet gericht zijn op het verwerken van persoonsgegevens, maar moet een ander doel hebben.

Soms heeft u toestemming nodig.

Let op dat u geen persoonsgegevens verwerkt die niet noodzakelijk zijn voor de uitvoering daarvan. Doet u dat wel? Dan moet u daarvoor rechtsgeldige toestemming of een andere grondslag hebben.

Voorbeeld: als u online een product verkoopt, moet u adresgegevens verwerken om het product bij iemand te kunnen bezorgen. Wilt u de persoonsgegevens daarnaast ook nog gebruiken om het koopgedrag van iemand te analyseren? Dan moet u hiervoor rechtsgeldige toestemming hebben van de betrokken persoon.

Verantwoordingsplicht

Zijn de persoonsgegevens echt noodzakelijk voor de naleving van de overeenkomst met ieder betrokken individu? Zorg ervoor dat u goed kunt onderbouwen dat u zich op deze grondslag mag baseren. Onder de AVG heeft u namelijk een verantwoordingsplicht.

3. Grondslag: Noodzakelijk voor het nakomen van een wettelijke verplichting

4. Grondslag: Noodzakelijk ter bescherming van vitale belangen

5. Grondslag: Noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag

6. Grondslag: Noodzakelijk voor de behartiging van de gerechtvaardigde belangen

Welke persoonsgegevens mag u verwerken

Wat wordt verstaan onder persoonsgegevens?

Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Mag u bijzondere persoonsgegevens verwerken?

De verwerking van bijzondere persoonsgegevens is verboden

Tenzij u zich kunt beroepen op een wettelijke uitzondering én één van de grondslagen voor het verwerken van 'gewone' persoonsgegevens.

Er zijn wettelijke uitzonderingen voor verwerkingen van bijzondere persoonsgegevens die strikt noodzakelijk en vanzelfsprekend zijn. Zoals voor het verwerken van medische gegevens door huisartsen en ziekenhuizen. Of voor het verwerken van lidmaatschap van een vakbond of politieke partij door die organisaties zelf.

Er zijn 10 wettelijke uitzonderingen op het verbod op het verwerken van bijzondere persoonsgegevens:

1. Uitdrukkelijke toestemming. Iemand kan uitdrukkelijke toestemming geven voor de verwerking van zijn of haar bijzondere persoonsgegevens voor het doel of de doelen die u heeft aangegeven;
2. Verwerkingen die noodzakelijk zijn voor de uitvoering van verplichtingen en het uitoefenen van arbeidsrecht en het sociale zekerheidsrecht zoals geregeld in de nationale wet;
3. Verwerkingen die noodzakelijk zijn om de vitale belangen te beschermen;
4. Verwerkingen voor gerechtvaardigde activiteiten door een instantie zonder winstoogmerk. De instantie moet wel passende waarborgen hebben ingebouwd en het mag alleen gaan om gegevensverwerkingen van (voormalige) leden of personen die regelmatig contact met de instantie onderhouden;
5. Verwerkingen van persoonsgegevens die door de betrokken personen zelf openbaar zijn gemaakt;
6. Verwerkingen die noodzakelijk zijn voor rechtsvordering of rechtsbevoegdheden;
7. Verwerkingen met een zwaarwegend algemeen belang. Daarbij moet u de evenredigheid en de inhoud van het recht op bescherming respecteren. Ook moet u de maatregelen treffen zoals geregeld in een nationale wet;
8. Verwerkingen die noodzakelijk voor de doelen gezondheidszorg, sociale diensten en arbeidsongeschiktheid, zoals geregeld in een nationale wet;
9. Verwerkingen die noodzakelijk zijn voor de volksgezondheid, zoals geregeld in een nationale wet;
10. Verwerkingen die noodzakelijk zijn voor archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statische doeleinden.

Wat verstaat de AVG onder bijzondere persoonsgegevens?

Persoonsgegevens die door hun aard bijzonder gevoelig zijn, krijgen ook onder de Algemene verordening gegevensbescherming (AVG) extra bescherming. Nieuw onder de AVG is dat ook genetische gegevens en biometrische gegevens hieronder vallen als deze herleidbaar zijn tot een persoon.

- De volgende persoonsgegevens ziet de AVG als bijzondere persoonsgegevens:
- Persoonsgegevens waaruit ras of etnische afkomst blijkt;
- Persoonsgegevens waaruit politieke opvattingen blijken;
- Persoonsgegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken;
- Persoonsgegevens waaruit het lidmaatschap van een vakvereniging blijkt;
- Gegevens over gezondheid;
- Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid;
- Genetische gegevens;
- Biometrische gegevens met het oog op de unieke identificatie van een persoon.

Genetische persoonsgegevens

Genetische persoonsgegevens geven unieke informatie over iemands fysiologie of gezondheid en/of over de gezondheid van familieleden. Dat maakt de informatie zo gevoelig.

In de praktijk gaat het hierbij vooral om informatie over erfelijkheid en genetische kenmerken die het

resultaat is van een biologisch monster. Bijvoorbeeld informatie uit analyse van het DNA.

Biometrische persoonsgegevens

Biometrische persoonsgegevens geven unieke informatie over iemands fysieke, fysiologische of gedragsgerelateerde kenmerken. Dat maakt het zo gevoelig.

In de praktijk gaat het hierbij vooral om biometrische persoonsgegevens die het resultaat zijn van een specifieke technische verwerking waardoor de gegevens tot een individu herleidbaar zijn. Zoals bij vingerafdrukgegevens.

Speciale regels voor strafrechtelijke persoonsgegevens

Let op: anders dan onder de Wet bescherming persoonsgegevens, zijn strafrechtelijke persoonsgegevens geen bijzondere persoonsgegevens. Voor strafrechtelijke persoonsgegevens gelden onder de AVG specifieke eisen.

Mag u strafrechtelijke persoonsgegevens verwerken?

Mag u onder de AVG persoonsgegevens van kinderen verwerken?

Rechten van betrokkenen

Onder de Algemene verordening gegevensbescherming (AVG) krijgen mensen meer mogelijkheden om voor zichzelf op te komen als hun persoonsgegevens worden verwerkt. Hun bestaande privacyrechten worden uitgebreid en er gelden 2 nieuwe rechten. Bent u klaar voor verzoeken van personen die hun rechten willen uitoefenen?

De AVG-privacyrechten

1. Het recht op dataportabiliteit. Het recht om persoonsgegevens over te dragen (NIEUW).
2. Het recht op vergetelheid. Het recht om ‘vergeten’ te worden (NIEUW).
3. Recht op inzage. Dat is het recht van mensen om de persoonsgegevens die u van hen verwerkt in te zien.
4. Recht op rectificatie en aanvulling. Het recht om de persoonsgegevens die u verwerkt te wijzigen.
5. Het recht op beperking van de verwerking: Het recht om minder gegevens te laten verwerken.
6. Het recht met betrekking tot geautomatiseerde besluitvorming en profilering. Oftewel: het recht op een menselijke blik bij besluiten.
7. Het recht om bezwaar te maken tegen de gegevensverwerking.

Ten slotte hebben mensen recht op duidelijke informatie over wat u met hun persoonsgegevens doet. Onder de AVG moet u aan een aantal specifieke eisen voldoen.

Bent u voorbereid?

U moet uw systemen, processen en interne organisatie op deze (nieuwe) rechten inrichten. Zodat u vanaf 25 mei 2018 op de juiste manier gehoor kunt geven aan verzoeken van mensen die hun rechten uitoefenen. Hieronder vindt u meer informatie over de verschillende rechten. En wanneer en hoe u daar gehoor aan moet geven.

Hoe bereidt u zich voor op de (nieuwe) privacyrechten van mensen?

Onder de Algemene verordening gegevensbescherming (AVG) worden de privacyrechten van personen versterkt en uitgebreid. U moet uw systemen, processen en interne organisatie op deze (nieuwe) rechten inrichten. Zodat u vanaf 25 mei 2018 op de juiste manier gehoor kunt geven aan verzoeken van betrokkenen.

Waar moet u op letten?

Om volgens de regels op een verzoek te reageren moet u het volgende weten en doen:

- Weet u en weten uw eventuele medewerkers welke privacyrechten er gelden en wanneer u wel of niet gehoor hoeft te geven aan een verzoek?
- Weet u en weten uw eventuele medewerkers hoe u aan de verzoeken gaat voldoen? Bijvoorbeeld: op welke manier u mensen inzage gaat geven, hun gegevens wist of gaat overdragen. Mogelijk moet u daarvoor technische en organisatorische maatregelen nemen;
- Wijst u mensen op de privacyrechten die zij hebben? Bijvoorbeeld via uw privacystatement?
- Informeert u mensen duidelijk over hóe zij een verzoek bij u kunnen indienen?
- Is het voor mensen makkelijk om een verzoek bij u te doen? Wanneer iemand elektronisch (bijvoorbeeld per e-mail) een verzoek doet, dan moet u de gevraagde informatie ook elektronisch geven.
- Kunt u zo snel mogelijk maar in ieder geval binnen 1 maand* reageren op een verzoek? Concreet betekent dit dat u binnen die termijn ofwel het verzoek moet hebben uitgevoerd en de verzoeker hierover hebben geïnformeerd, of hebben aangegeven waarom u geen gehoor geeft aan het verzoek.

In uitzonderlijke gevallen mag u binnen 3 maanden reageren op een verzoek. Bijvoorbeeld wanneer een verzoek heel complex is. Of wanneer het aantal ontvangen verzoeken van dezelfde persoon extreem hoog is. Maar ook dan geldt dat u wel binnen 1 maand moet laten weten dat u meer tijd nodig heeft om op het verzoek te reageren.

Kosten

U mag in principe géén kosten berekenen. Maar kunt u bewijzen dat een verzoek ongegrond of buitensporig is? Bijvoorbeeld omdat iemand heel veel verzoeken bij u indient? Dan mag u een redelijke administratieve vergoeding vragen. Of het verzoek weigeren.

1. Het recht op dataportabiliteit.

2. Het recht op vergetelheid (wissing van gegevens)

Wat houdt het recht op vergetelheid uit de AVG in?

In Artikel 17 van de Algemene verordening gegevensbescherming (AVG) is het zogeheten recht op vergetelheid opgenomen. Dit recht houdt in dat organisaties in een aantal gevallen persoonsgegevens moeten wissen als een betrokkene (diegene van wie de organisatie gegevens verwerkt) erom vraagt.

Voorwaarden recht op vergetelheid

Het recht op vergetelheid geldt niet altijd. Alleen in de volgende situaties is het recht op vergetelheid van toepassing:

- Niet meer nodig
- De organisatie heeft de persoonsgegevens niet meer nodig voor de doeleinden waarvoor de organisatie ze heeft verzameld of waarvoor de organisatie ze verwerkt.
- Intrekken toestemming
- De betrokkene heeft eerder (uitdrukkelijke) toestemming gegeven aan de organisatie voor het gebruik van zijn gegevens, maar trekt die toestemming nu in.
- Bezwaar
- De betrokkene maakt bezwaar tegen de verwerking. Er geldt op grond van artikel 21 van de AVG een absoluut recht van bezwaar tegen direct marketing. En een relatief recht van bezwaar als de rechten van de betrokkene zwaarder wegen dan het belang van de organisatie om de persoonsgegevens te verwerken.

- Onrechtmatige verwerking
- De organisatie verwerkt de persoonsgegevens onrechtmatig. Bijvoorbeeld omdat er geen wettelijke grondslag is voor de verwerking.
- Wettelijk bepaalde bewaartermijn
- De organisatie is wettelijk verplicht om de gegevens na bepaalde tijd te wissen.
- Kinderen
- De betrokkene is jonger dan 16 jaar en de persoonsgegevens zijn verzameld via een app of website ('dienst van de informatiemaatschappij').

Verschil met nu

Het recht op vergetelheid lijkt op het huidige recht op correctie en verwijdering (artikel 36 van de Wet bescherming persoonsgegevens). Maar het recht op vergetelheid is breder. Het recht is niet meer – zoals nu – beperkt tot het verwijderen van objectief onjuiste gegevens, onvolledige gegevens of niet ter zake doende gegevens.

Wanneer geldt het recht op vergetelheid uit de AVG niet?

De Algemene verordening gegevensbescherming (AVG) noemt een aantal omstandigheden waarin het recht op vergetelheid niet geldt:

- De verwerking is noodzakelijk om het recht op vrijheid van meningsuiting en informatie uit te oefenen. Daarmee doet de AVG recht aan het principe dat privacy en vrijheid van meningsuiting gelijkwaardige grondrechten zijn.
- De organisatie verwerkt de gegevens omdat er een wettelijke verplichting is om dat te doen.
- De organisatie verwerkt de gegevens om openbaar gezag of een (wettelijk vastgelegde) taak van algemeen belang uit te oefenen.
- De organisatie verwerkt de gegevens voor een taak van algemeen belang op het gebied van de volksgezondheid.
- De organisatie moet de gegevens in het algemeen belang archiveren.
- De gegevens zijn noodzakelijk voor een rechtsvordering.

Algemene uitzonderingen privacyrechten

Daarnaast is in artikel 23 van de AVG een aantal algemene uitzonderingen opgenomen op de rechten van betrokkenen. Dit artikel lijkt op het huidige artikel 43 van de Wet bescherming persoonsgegevens.

Het artikel biedt organisaties de mogelijkheid om in bijzondere omstandigheden geen gehoor te geven aan verzoeken van betrokkenen. Zij moeten dan voor dat verzoek een belangenafweging maken waaruit blijkt dat hun belangen (of de rechten en vrijheden van anderen) zwaarder wegen dan het privacyrecht van de betrokkene.

Het is bijvoorbeeld niet de bedoeling dat betrokkenen met een beroep op hun rechten sporen van crimineel gedrag wissen.

Wat moet ik als organisatie doen als ik een verzoek krijg om gegevens te wissen?

Zodra de Algemene verordening gegevensbescherming (AVG) geldt, hebben betrokkenen (degenen van wie u gegevens verwerkt) het recht op vergetelheid. Vraagt iemand u op grond van dit recht om zijn gegevens te wissen? Dan moet u dat onmiddellijk doen, uiterlijk binnen een maand. Alleen als het om een heel complex verzoek gaat, heeft u twee maanden extra de tijd. U moet dan wel binnen een maand aan de betrokkene laten weten dat het langer gaat duren.

Manier van reageren

Als een betrokkene het verzoek elektronisch indient, moet u ook elektronisch reageren. Tenzij de betrokkene u vraagt om op een andere manier te reageren.

Kosten

U mag in principe géén kosten berekenen. Maar kunt u bewijzen dat een verzoek ongegrond of buitensporig is (veelvuldig herhaalde verzoeken van één persoon)? Dan mag u een redelijke administratieve vergoeding vragen. Of het verzoek weigeren.

Derde partijen informeren

Heeft u de betreffende persoonsgegevens aan derde partijen verstrekt? Dan moet u die ontvangers informeren dat u deze persoonsgegevens heeft gewist. En uitleggen dat ook de ontvangers iedere kopie van of koppeling naar die persoonsgegevens moeten wissen.

Publiceert u bijvoorbeeld persoonsgegevens via een website? Dan moet u zoekmachines informeren. U kunt daarbij de webpagina opnieuw laten indexeren, zodat de gewiste persoonsgegevens niet meer verschijnen in de zoekresultaten.

Als een betrokkene erom vraagt, moet u ook vertellen welke ontvangers u op die manier heeft geïnformeerd (artikel 19 van de AVG).

Vallen back-ups ook onder het recht op vergetelheid?

Ja. U moet het recht op vergetelheid ook toepassen op digitale back-upbestanden. Vraagt iemand u om zijn gegevens te wissen? Dan moet u zijn persoonsgegevens dus ook zo snel mogelijk uit uw back-ups verwijderen.

Zodra de Algemene verordening gegevensbescherming (AVG) geldt, hebben mensen het recht op vergetelheid. Dit houdt in dat u in bepaalde gevallen verplicht bent om iemands gegevens te verwijderen als diegene hierom vraagt. Bijvoorbeeld als de gegevens niet meer nodig zijn of als die persoon zijn toestemming intrekt.

Eisen aan back-ups

Zo gaat u goed om met back-ups onder de AVG:

- Inventariseer van welke gegevens u back-ups moet bijhouden, bijvoorbeeld vanwege uw beveiligingsbeleid. Houd er rekening mee dat u alleen gegevens mag verwerken die noodzakelijk zijn voor het doel van uw verwerking (zie artikel 5 van de AVG). U moet ook kunnen aantonen dat deze gegevens noodzakelijk zijn. Dat is onderdeel van uw verantwoordingsplicht.
- Maak regelmatig back-ups en verwijder systematisch verouderde gegevens.
- Informeer mensen goed over welke aanvullende bewaartermijn noodzakelijk is voor back-ups van uw specifieke dienstverlening. Bijvoorbeeld: u bewaart persoonsgegevens van klanten 1 jaar in uw reguliere systemen, maar hanteert aanvullend een bewaartermijn van 3 maanden voor uw back-ups.
- Richt uw back-upsysteem zo in dat u verwijderverzoeken van betrokkenen ook kan doorvoeren in dit systeem.
- Is het noodzakelijk voor uw dienstverlening om back-ups te maken die moeilijk of niet overschrijfbaar zijn, zoals tapes? Dan kunt u de persoonsgegevens niet verwijderen uit de back-ups. Zorg dan wel dat u goed bijhoudt welke persoonsgegevens u had moeten verwijderen. Is het onverhoopt nodig om een back-up terug te zetten? Dan moet u deze gegevens alsnog verwijderen.

Uitzonderingen

Er zijn ook uitzonderingen op het recht op vergetelheid. U hoeft de betreffende persoonsgegevens bijvoorbeeld niet uit uw back-ups te verwijderen als u wettelijk verplicht bent om de gegevens een bepaalde tijd te bewaren. Of als u ze moet archiveren in het algemeen belang.

3. Het recht op inzage

Wat houdt het recht op inzage in?

De Algemene verordening gegevensbescherming (AVG) geeft mensen meer zeggenschap over hun persoonsgegevens. Ze hebben het recht om u te vragen welke gegevens u van hen heeft. Ze mogen u ook vragen deze gegevens in te zien. In de AVG (artikel 15) staat dit recht beschreven als ‘recht op inzage’.

Bij inzageverzoeken moet u ook laten weten:

- Waarom u bepaalde gegevens verwerkt.
- Welke soorten persoonsgegevens u verzamelt.
- Indien van toepassing: aan welke organisaties u de persoonsgegevens doorgeeft. Dit geldt ook voor gegevens die u doorgeeft aan organisaties in andere landen of aan internationale organisaties.
- Hoe lang u de persoonsgegevens bewaart. Als u dat niet precies kunt aangeven, moet u duidelijk kunnen maken welke criteria u hanteert om een bewaartermijn te bepalen.
- Welke privacyrechten mensen hebben: het recht om hun persoonsgegevens te laten wijzigen, aanvullen of wissen, om u te vragen om minder persoonsgegevens te verwerken en om bezwaar te maken als u hun persoonsgegevens verwerkt.
- Dat mensen het recht hebben om een klacht in te dienen bij de Autoriteit Persoonsgegevens.
- Indien van toepassing: van welke organisatie u persoonsgegevens heeft ontvangen als u deze niet zelf heeft verzameld bij de betrokken personen.
- Indien van toepassing: op basis van welke logica u een geautomatiseerd besluit over iemand neemt.

4. Het recht op rectificatie

5. Recht op beperking van de verwerking

6. Het recht van bezwaar

7. Het recht op informatie

Privacyverklaring

Hoe stelt u een privacyverklaring op?

De AVG stelt een aantal specifieke eisen waar een privacyverklaring aan moet voldoen. Deze eisen gaan over de inhoud, de toegankelijkheid en de duidelijkheid van de informatie.

Welke informatie moet er in een privacyverklaring staan?

In het document moet u in ieder geval de volgende informatie geven:

- De identiteit en de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van uw vertegenwoordiger in de EU;
- De contactgegevens van de FG als u die heeft.
- De doeleinden en rechtsgrond van de verwerking, en als u zich beroept op een gerechtvaardigd belang: op welk belang u zich beroept.
- De (categorieën van) ontvangers van de persoonsgegevens.
- Of u van plan bent de persoonsgegevens door te geven buiten de EU of een internationale organisatie en op welke juridische grond.
- De bewaartermijn van de gegevens.

- De rechten van de betrokkene, zoals het recht op inzage, correctie en verwijdering. Zie ook stap 10.
- Het recht van de betrokkene om de gegeven toestemming voor een bepaalde verwerking altijd in te kunnen trekken.
- Dat de betrokkene een klacht kan indienen bij de relevante privacytoezichthouder.
- Of en waarom de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de gevolgen zijn als de gegevens niet worden verstrekt.
- Of u gebruik maakt van geautomatiseerde besluitvorming, inclusief profilering, en hoe u besluiten neemt.
- Als de gegevens van een andere organisatie zijn verkregen: de bron waar de persoonsgegevens vandaan komen, en in voorkomend geval, of zij afkomstig zijn van openbare bronnen.

Hoe zorgt u dat u privacyverklaring toegankelijk is?

In de AVG staat dat u de informatie over uw verwerkingen in principe schriftelijk moet geven. De beste manier om er zeker van te zijn dat uw informatie voor de meeste mensen goed vindbaar is, is het publiceren van een online privacyverklaring.

Daarnaast mag u andere middelen inzetten om de inhoud van uw privacybeleid toegankelijk te maken. Zoals het tonen van pop-ups met een toelichting bij elke toestemmingsvraag. Of het gebruik van iconen of een video.

Tip: om de informatie in een (online) privacyverklaring zo toegankelijk mogelijk te maken, kunt u de verklaring in meerdere lagen opstellen. Bijvoorbeeld:

- In de eerste laag geeft u kort aan wie de verantwoordelijke organisatie is, hoe die te bereiken is en welke gegevensverwerkingen de meeste impact hebben op de betrokken personen.
- In de tweede en derde laag van de privacyverklaring kunt u meer in detail aangeven welke persoonsgegevens u voor welk doel verwerkt en hoe mensen hun rechten kunnen uitoefenen.

Duidelijke taal

De informatie over de gegevensverwerking moet beknopt, transparant en begrijpelijk zijn. Daarom moet u duidelijke en eenvoudige taal gebruiken.

Dat betekent onder meer: wees kort en bondig,vermijd vaktermen en verplaats u in de lezer.

Richt u zich tot kinderen onder de zestien jaar? Of weet u dat kinderen uw diensten veel gebruiken? Dan moet u de woordkeuze, toon en stijl van de informatie aanpassen. Zodat de kinderen weten dat deze informatie voor hen is bedoeld en ze de informatie kunnen begrijpen.

Verantwoordingsplicht

De Algemene verordening gegevensbescherming (AVG) legt meer verantwoordelijkheid bij u als organisatie om aan te tonen dat u aan de privacyregels voldoet. Door te voldoen aan uw verantwoordingsplicht (accountability) levert u een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy.

De nieuwe regels dwingen u om goed na te denken over hoe uw organisatie persoonsgegevens verwerkt en beschermt. De verantwoordingsplicht houdt in dat u moet kunnen aantonen dat uw verwerkingen aan de regels van de AVG voldoen.

U moet bijvoorbeeld kunnen aantonen dat een verwerking aan de belangrijkste beginselen van verwerking voldoet, zoals:

- rechtmatigheid;
- transparantie;

- doelbinding;
- juistheid.

Ook moet u kunnen laten zien dat u de juiste technische en organisatorische maatregelen hebt genomen om de persoonsgegevens te beschermen.

U bent verplicht verantwoording af te leggen over uw gegevensverwerkingen wanneer de Autoriteit Persoonsgegevens daar om vraagt. Zorg daarom dat u aan uw verantwoordingsplicht voldoet vanaf 25 mei 2018. Vanaf dan geldt de AVG.

Hoe voldoe ik aan de verantwoordingsplicht?

In de Algemene verordening gegevensbescherming (AVG) staan een aantal verplichte maatregelen genoemd waarmee u aan uw verantwoordingsplicht (accountability) voldoet. Naast de verplichte maatregelen kunt u ervoor kiezen om extra maatregelen te nemen.

Verplichte maatregelen

De verplichte maatregelen die de AVG concreet noemt zijn:

- het bijhouden van een register van verwerkingsactiviteiten;
- het uitvoeren van een data protection impact assessment (DPIA) voor gegevensverwerkingen met een hoog privacyrisico;
- het bijhouden van een register van datalekken die zijn opgetreden;
- het aantonen dat een betrokkene daadwerkelijk toestemming heeft gegeven voor een gegevensverwerking wanneer u voor een verwerking toestemming nodig heeft.
- wanneer onduidelijk is of u verplicht bent om een Functionaris voor gegevensbescherming aan te stellen, moet u goed kunnen onderbouwen waarom u ervoor gekozen hebt om al dan niet een FG aan te stellen.

Meer informatie over deze verplichtingen vindt u in het AVG-dossier van de autoriteit persoonsgegevens (AP)en in de AVG zelf.

Extra maatregelen

Naast de verplichte maatregelen kunt u ervoor kiezen om extra maatregelen te nemen waarmee u aantoont dat u voldoet aan de eisen van de AVG. Bijvoorbeeld:

- het aansluiten bij een gedragscode;
- het behalen van een bepaald certificaat;
- het hanteren van een specifiek ICT-beveiligingsbeleid;
- het afleggen van verantwoording over de verwerking van persoonsgegevens in uw jaarverslag of in een speciaal privacy-jaarverslag.

Hoewel deze maatregelen niet verplicht zijn, helpen zij u wel om aan de toezichthouder te laten zien dat u voldoet aan de eisen van de AVG. Daarom moedigen wij deze vrijwillige maatregelen aan.

Ben ik verplicht om een register van verwerkingsactiviteiten op te stellen?

Het opstellen van een register van verwerkingsactiviteiten is onder de AVG vaak een verplichte maatregel. In het register staat informatie over de persoonsgegevens die u verwerkt. Of u zo'n register moet opstellen, hangt af van de omvang van uw organisatie en het type gegevens dat u verwerkt.

Let op: In de praktijk is vrijwel iedere organisatie verplicht een verwerkingsregister bij te houden!

Organisaties met meer dan 250 medewerkers

Heeft uw organisatie meer dan 250 medewerkers? Dan bent u verplicht om een register van verwerkingsactiviteiten bij te houden.

Organisaties met minder dan 250 medewerkers

Heeft uw organisatie minder dan 250 medewerkers? Dan moet u over een register beschikken wanneer u persoonsgegevens verwerkt:

- waarvan de verwerking niet incidenteel is. In de praktijk zijn verwerkingen zelden incidenteel. Denk bijvoorbeeld aan de persoonsgegevens van medewerkers die u verwerkt. Of van uw klanten, cliënten, patiënten of inwoners en/of;
- die een hoog risico inhouden voor de rechten en vrijheden van de personen van wie u persoonsgegevens verwerkt en/of;
- die vallen onder de categorie bijzondere persoonsgegevens. Zoals gegevens over godsdienst, gezondheid en politieke voorkeur of strafrechtelijke gegevens.

Bent u verplicht om een register van verwerkingsactiviteiten op te stellen? Dan moet u dit register kunnen verstrekken wanneer de Autoriteit Persoonsgegevens daar om vraagt.

Wat moet er in het register van verwerkingsactiviteiten staan?

Aantonen gegeven toestemming

Verwerkersovereenkomst

Wanneer moet u een verwerkersovereenkomst opstellen?

Als u andere partijen inschakelt om persoonsgegevens voor u te verwerken, moet u met deze organisaties een 'verwerkersovereenkomst' afsluiten. Met een verwerkersovereenkomst sluit u uit dat de andere partij de persoonsgegevens voor eigen doelen mag verwerken.

U mag alleen verwerkers inschakelen die voldoende garanties bieden dat zij aan de wettelijke vereisten voldoen. Maar let op: als u de gegevensverwerking door een verwerker laat uitvoeren, dan bent u nog steeds verantwoordelijk voor de naleving van de Algemene verordening gegevensbescherming (AVG).

Wat moet er in een verwerkersovereenkomst staan?

In de overeenkomst legt u onder meer het volgende vast:

- Het onderwerp en de duur van de gegevensverwerking.
- De aard en het doel van de gegevensverwerking.
- Het soort persoonsgegevens.
- De categorieën van betrokkenen.
- De rechten en verplichtingen van de verwerkingsverantwoordelijke.

Wat moet er in een verwerkersovereenkomst staan?

Maakt u, zodra de Algemene verordening gegevensbescherming (AVG) geldt, gebruik van de diensten van een verwerker (nu nog ‘bewerker’ genoemd)? Dan zijn u en de verwerker verplicht om een aantal onderwerpen vast te leggen in een schriftelijke overeenkomst (zie artikel 28, lid 3 van de AVG).

U moet de volgende onderwerpen vastleggen:

Algemene beschrijving

- Een omschrijving van het onderwerp, de duur, de aard en het doel van de verwerking, het soort

persoonsgegevens, de categorieën van betrokkenen en uw rechten en verplichtingen als verwerkingsverantwoordelijke (nu nog 'verantwoordelijke' genoemd).

Instructies verwerking

- De verwerking vindt in principe uitsluitend plaats op basis van uw schriftelijke instructies. De verwerker mag de persoonsgegevens niet voor eigen doeleinden gebruiken.

Geheimhoudingsplicht

- Personen in dienst van of werkzaam voor de verwerker hebben een geheimhoudingsplicht.

Beveiliging

- De verwerker treft passende technische en organisatorische maatregelen om de verwerking te beveiligen. Bijvoorbeeld pseudonimisering en versleuteling van persoonsgegevens, permanente informatiebeveiliging, herstel van beschikbaarheid en toegang tot gegevens bij incidenten, regelmatige beveiligingstesten.

Subverwerkers

- De verwerker schakelt geen subverwerker(s) in zonder uw voorafgaande schriftelijke toestemming. De verwerker legt aan een subverwerker in een subverwerkersovereenkomst dezelfde verplichtingen op als de verwerker richting u heeft.
- In de overeenkomst kunt u ook direct afspreken dat, en onder welke voorwaarden, de verwerker subverwerkers mag inschakelen.
- Komt de subverwerker zijn verplichtingen niet na? Dan blijft de verwerker volledig aansprakelijk richting u voor het nakomen van de verplichtingen van de subverwerker (zie artikel 28, lid 4 van de AVG).

Privacyrechten

- De verwerker helpt u om te voldoen aan uw plichten als betrokkenen hun privacyrechten uitoefenen (zoals het recht op inzage, correctie, vergetelheid en dataportabiliteit).

Andere verplichtingen

- De verwerker helpt u ook om andere verplichtingen na te komen. Zoals bij het melden van datalekken, het uitvoeren van een data protection impact assessment (DPIA) en bij een voorafgaande raadpleging.

Gegevens verwijderen

- Na afloop van de verwerkingsdiensten verwijdert de verwerker de gegevens. Of bezorgt hij deze aan u terug, als u dat wilt. Ook verwijdert hij kopieën. Tenzij de verwerker wettelijk verplicht is de gegevens te bewaren.

Audits

- De verwerker werkt mee aan uw audits of die van een derde partij. En stelt alle relevante informatie beschikbaar om te kunnen controleren of hij zich als verwerker houdt aan de hierboven genoemde verplichtingen (uit artikel 28 AVG).

Gegevensbeschermingsbeleid

Wanneer is een gegevensbeschermingsbeleid volgens de AVG verplicht?

U bent alleen verplicht om een gegevensbeschermingsbeleid op te stellen als dat in verhouding staat tot uw verwerkingsactiviteiten. Een gegevensbeschermingsbeleid wordt ook wel privacybeleid genoemd. Of u verplicht bent om zo'n privacybeleid op te stellen, hangt af van de concrete omstandigheden. Zoals de aard, de omvang, de context en het doel van de gegevensverwerking.

Ziekenhuizen, gemeenten, social mediabedrijven en handelsinformatiebureaus zullen daarom vaak verplicht zijn om een gegevensbeschermingsbeleid op te stellen. Ook kleine organisaties kunnen verplicht zijn een gegevensbeschermingsbeleid op te stellen.

Vrijwillig opstellen van een gegevensbeschermingsbeleid

Bent u niet verplicht om een gegevensbeschermingsbeleid op te stellen? Dan kan het toch nuttig zijn om dat wél te doen. Het helpt u namelijk om te zien of u voldoende maatregelen heeft genomen om de persoonsgegevens van uw klanten, patiënten, cliënten e.d. te beschermen. Daarnaast is het een manier waarmee u aan zowel uw doelgroep als de Autoriteit Persoonsgegevens kunt laten zien dat u voldoet aan de AVG.

Let op: een gegevensbeschermingsbeleid is iets anders dan een privacyverklaring. Alle organisaties die persoonsgegevens verwerken, moeten mensen heldere informatie geven over de persoonsgegevens die zij verwerken en voor welk(e) doel(en) zij deze gegevens verwerken. De meest aangewezen manier hiervoor is het opstellen van een online privacyverklaring.

Wat moet er volgens de AVG in een gegevensbeschermingsbeleid staan?

In de Algemene verordening gegevensbescherming (AVG) staat niet precies omschreven welke gegevens u in uw gegevensbeschermingsbeleid (ook wel privacybeleid genoemd) moet opnemen. Uit het beleid moet in ieder geval wèl blijken hoe u voldoet aan de AVG. Dat is onderdeel van uw verantwoordingsplicht.

Informatie gegevensbeschermingsbeleid

U kunt laten zien hoe u voldoet aan de AVG door onder andere deze informatie op te nemen:

- een omschrijving van de categorieën persoonsgegevens die u verwerkt;
- een beschrijving van de doeleinden waarvoor u persoonsgegevens verwerkt en wat de juridische grondslag daarvan is;
- hoe u voldoet aan de beginselen van verwerking van persoonsgegevens. Zoals de verplichting om niet meer gegevens te verwerken dan noodzakelijk;
- welke rechten betrokkenen hebben en hoe zij die rechten kunnen uitoefenen. Zoals het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Maar ook het recht op inzage, wijzigen, wissen en het ontvangen van alle geregistreerde gegevens;
- welke organisatorische en technische maatregelen u genomen heeft om de persoonsgegevens te beveiligen;
- hoe lang u de persoonsgegevens bewaart.

Het opstellen van een gegevensbeschermings- of privacybeleid is niet altijd verplicht. Toch kan het nuttig zijn om zo'n beleid wel op te stellen.

Beveiligen van persoonsgegevens en verwerkingen

Gedragscodes

Datalekken

Of u een datalek moet melden aan de toezichthouder (AP) en de betrokkene die het betreft, is

afhankelijk van het risico van de inbreuk voor de betrokkene en of er aan bepaalde voorwaarden is voldaan. De voorwaarden voor het melden aan de toezichthouder en de betrokkene verschillen onderling. Voor het melden staat een maximale wettelijke termijn en de melding moet bepaalde informatie bevatten.

Belangrijk en nieuw is dat u i**eder datalek moet registreren** en dat u zich daarover op afroep direct moet kunnen verantwoorden naar de toezichthouder. Het beschikbaar hebben van de informatie over ieder datalek maakt onderdeel uit van de verantwoordingsplicht.

Wanneer moet u een datalek (inbreuk) melden bij de toezichthouder (AP)?

Wanneer moet u een datalek (inbreuk) mededelen aan een betrokkene die het betreft?

Data protection impact assessment (DPIA)

Per 25 mei 2018 geldt de Algemene verordening gegevensbescherming (AVG). Vanaf dit moment kunnen organisaties verplicht zijn een data protection impact assessment (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

In de Nederlandse vertaling van de AVG wordt de term data protection impact assessment (DPIA) gegevensbeschermingseffectbeoordeling genoemd.

Groot privacyrisico

Organisaties hoeven, zodra de AVG geldt, niet voor elke gegevensverwerking een DPIA uit te voeren. Een DPIA is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen (de mensen van wie de organisatie gegevens verwerkt). Dat is in ieder geval zo als een organisatie:

1. systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profiling;
2. op grote schaal bijzondere persoonsgegevens verwerkt;
3. op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

Buiten deze drie situaties geeft de AVG geen overzicht van verwerkingen met een hoog risico. De Europese privacytoezichthouders hebben criteria opgesteld om het risico te bepalen. Daarnaast publiceert de Autoriteit Persoonsgegevens (AP) op termijn een lijst van verwerkingen waarvoor een DPIA verplicht is.

Guidelines DPIA

De Europese privacytoezichthouders hebben in oktober 2017 de (definitieve) Guidelines on Data Protection Impact Assessment gepubliceerd die meer uitleg geven over de DPIA. Er is ook een officiële Nederlandse vertaling van de guidelines DPIA beschikbaar.

Huidige situatie

De Rijksoverheid is nu al verplicht om bij de ontwikkeling van nieuwe wetgeving rekening te houden met de resultaten van een DPIA, nu nog Privacy Impact Assessment (PIA) genoemd. Andere organisaties zijn nu nog niet maar vanaf 25 mei 2018 verplicht een (D)PIA uit te voeren.

Het is aan te raden om vrijwillig een (D)PIA te doen. Dit komt niet alleen de gegevensbescherming ten goede, maar ook voor de organisatie zelf levert een (D)PIA voordelen op.

In welke gevallen moet ik een DPIA uitvoeren?

Als verantwoordelijke moet u een data protection impact assessment (DPIA) uitvoeren wanneer uw gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert. Dit moet u zelf bepalen. De werkgroep van Europese privacytoezichthouders (WP29) heeft een lijst van 9* criteria opgesteld om u hierbij te helpen.

9 criteria om te toetsen of u een DPIA moet uitvoeren

Als vuistregel kunt u hanteren dat u een DPIA moet uitvoeren als uw verwerking aan 2 of meer van de onderstaande 9 criteria voldoet.

1. Beoordelen van mensen op basis van persoonskenmerken

Het gaat hierbij onder meer om profiling en het maken van prognoses, met name op basis van kenmerken als iemands beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen.

Voorbeelden hiervan zijn een bank die de kredietwaardigheid van klanten bepaalt (creditscoring), een bedrijf dat DNA-testen aan consumenten levert om gezondheidsrisico's te testen en een bedrijf dat bezoekers van zijn website volgt en op basis daarvan profielen van deze mensen opstelt.

2. Geautomatiseerde beslissingen

Het gaat hierbij om beslissingen die voor de betrokkene rechtsgevolgen of vergelijkbare wezenlijke gevolgen hebben. Zo'n gegevensverwerking kan er bijvoorbeeld toe leiden dat mensen worden uitgesloten of gediscrimineerd.

Gegevensverwerkingen met geringe of geen gevolgen voor mensen vallen niet onder dit criterium. In de aankomende WP29-guidelines over profiling volgt hierover meer uitleg.

3. Stelselmatige en grootschalige monitoring

Het gaat hierbij om monitoring van openbaar toegankelijke ruimten, bijvoorbeeld met cameratoezicht. Hierbij kunnen persoonsgegevens worden verzameld zonder dat betrokkenen weten wie hun gegevens verzamelt en wat daar vervolgens mee gebeurt. Bovendien kan het onmogelijk zijn voor mensen om zich in openbare ruimten aan deze gegevensverwerking te onttrekken.

4. Gevoelige gegevens

Het gaat hierbij om bijzondere categorieën van persoonsgegevens (zie artikel 9 van de AVG), zoals informatie over iemands politieke voorkeuren. Ook strafrechtelijke gegevens vallen hieronder. Tot slot gaat het hier ook om gegevens die over het algemeen als privacygevoelig worden beschouwd, zoals gegevens over elektronische communicatie, locatiegegevens en financiële gegevens.

5. Grootschalige gegevensverwerkingen

De AVG geeft geen definitie van 'grootschalige gegevensverwerkingen'. WP29 adviseert om met de volgende criteria te bepalen of hiervan sprake is:

- de hoeveelheid mensen van wie gegevens worden verwerkt;
- de hoeveelheid gegevens en/of de verscheidenheid aan gegevens die worden verwerkt;
- de tijdsduur van de gegevensverwerking;
- de geografische reikwijdte van de gegevensverwerking.

In de AVG staat niet precies uitgelegd wat 'grootschalig' inhoudt. Wel geven de Europese toezichthouders een aantal voorbeelden van verwerkingen die zij als grootschalig zien.

- Bijvoorbeeld een ziekenhuis dat patiëntgegevens verwerkt of een bank die klantgegevens verwerkt als onderdeel van de gebruikelijke werkzaamheden.
- Verwerking van bijzondere persoonsgegevens door individuele artsen of advocaten ('eenpitters'),

zien de AP en de andere Europese privacytoezichthouders niet als een grootschalige verwerking.

6. Gekoppelde databases

Het gaat hierbij om gegevensverzamelingen die aan elkaar gekoppeld of met elkaar gecombineerd zijn. Bijvoorbeeld databases die voortkomen uit twee of meer verschillende gegevensverwerkingen met verschillende doelen en/of uitgevoerd door verschillende verantwoordelijken, op een manier die betrokkenen niet redelijkerwijs kunnen verwachten.

7. Gegevens over kwetsbare personen

Bij het verwerken van dit type gegevens kan een DPIA nodig zijn omdat er sprake is van een ongelijke machtsverhouding tussen de betrokkene en de verantwoordelijke. Dit heeft als gevolg dat betrokkenen niet in vrijheid toestemming kunnen geven of weigeren voor het verwerken van hun gegevens. Het kan hierbij om bijvoorbeeld werknemers, kinderen en patiënten gaan.

8. Gebruik van nieuwe technologieën

De AVG is er duidelijk over dat een DPIA nodig kan zijn bij het gebruik van een nieuwe technologie. De reden hiervoor is dat dit gebruik gepaard kan gaan met nieuwe manieren om gegevens te verzamelen en gebruiken, met mogelijk grote privacyrisico's.

De persoonlijke en maatschappelijke gevolgen van het gebruik van een nieuwe technologie kunnen zelfs nog onbekend zijn. Een DPIA helpt de verantwoordelijke dan om de risico's te begrijpen en te verhelpen. Sommige 'Internet of Things'-toepassingen bijvoorbeeld kunnen een grote impact hebben op het dagelijks leven en de privacy van mensen, waardoor hierbij een DPIA nodig is.

9. Blokkering van een recht, dienst of contract

Het gaat hierbij om gegevensverwerkingen die tot gevolg hebben dat betrokkenen:

- een recht niet kunnen uitoefenen of;
- een dienst niet kunnen gebruiken of;
- een contract niet kunnen afsluiten.
- Bijvoorbeeld een bank die persoonsgegevens verwerkt om te bepalen of zij een lening aan iemand willen verstrekken.

Verantwoordingsplicht

Let op: deze 9 criteria zijn een handreiking om in te schatten of u een DPIA moet uitvoeren.**Ook als u aan slechts één of geen van deze criteria voldoet, moet u goed kunnen onderbouwen waarom u ervoor kiest om geen DPIA uit te voeren. Dit maakt onderdeel uit van de verantwoordingsplicht.**

*In de definitieve guidelines die zijn vastgesteld in oktober 2017, is het 10e criterium 'Doorgifte van persoonsgegevens buiten de EU' vervallen. Ook legt de wet voor bestaande verwerkingen nu een link naar het 'voorafgaand onderzoek' onder de huidige privacywetgeving.

Wanneer hoef ik geen DPIA uit te voeren?

U hoeft geen data protection impact assessment (PIA) uit te voeren wanneer uw gegevensverwerking:

- Waarschijnlijk geen hoog privacyrisico oplevert.
- Sterk lijkt op een andere gegevensverwerking waarvoor al een DPIA is uitgevoerd.
- Wordt geregeld door een andere Europese of nationale wet en er bij de totstandkoming van deze wet al een DPIA is uitgevoerd. Tenzij de privacytoezichthouder oordeelt dat er toch een DPIA nodig is.
- Op een lijst staat van verwerkingen waarvoor een DPIA niet verplicht is. De AVG geeft de privacytoezichthouder de mogelijkheid om zo'n lijst op te stellen, maar dit is niet verplicht.

Moet ik alsnog een DPIA uitvoeren voor een bestaande verwerking?

Ja, soms moet u alsnog een data protection impact assessment (DPIA) uitvoeren voor een bestaande verwerking. Dat is als er iets verandert aan het risico van de gegevensverwerking. En de gegevensverwerking vervolgens (na de verandering) een hoog privacyrisico oplevert.

Geen DPIA nodig

U hoeft dus niet alsnog een DPIA uit te voeren als een van de volgende 3 situaties van toepassing is:

- uw gegevensverwerking levert waarschijnlijk géén hoog privacyrisico op; of
- u heeft voor deze verwerking al eens een voorafgaand onderzoek door de AP laten uitvoeren en de verwerking is in de tussentijd niet veranderd; of
- de risico's van de verwerking zijn niet veranderd.
- Verwerking verandert

Uw verwerking verandert bijvoorbeeld als u een nieuwe technologie gaat gebruiken. Of als u persoonsgegevens voor een ander doel gaat gebruiken. In deze situaties verandert uw gegevensverwerking feitelijk in een nieuwe gegevensverwerking. En dan kan een DPIA verplicht zijn.

Risico verandert

Verandert het privacyrisico van uw verwerking? Dan kunt u ook verplicht zijn alsnog een DPIA uit te voeren. Risico’s kunnen bijvoorbeeld veranderen omdat een onderdeel van het verwerkingsproces wijzigt. De technologische ontwikkelingen gaan snel, waardoor nieuwe kwetsbaarheden kunnen ontstaan.

Omgeving verandert

Tot slot kunt u alsnog verplicht zijn een DPIA uit te voeren omdat de organisatie- of maatschappelijke context verandert. Bijvoorbeeld omdat de gevolgen van bepaalde geautomatiseerde beslissingen belangrijker zijn geworden of omdat er nieuwe categorieën mensen kwetsbaar worden voor discriminatie.

Periodieke DPIA

Vanwege de hierboven genoemde veranderingen is het sowieso aan te raden om periodiek een DPIA uit te voeren. Ook als de gegevensverwerking zelf niet is veranderd. Bijvoorbeeld een keer per 3 jaar.

Op welk moment moet ik een DPIA uitvoeren

Start met het data protection impact assessment (DPIA) zo vroeg als praktisch gezien mogelijk is in de ontwerpfase van de gegevensverwerking. Ook als nog niet alle details van de verwerking bekend zijn. Door vroeg te beginnen, is het voor u makkelijker om aan de wettelijk vereiste principes van privacy by design en privacy by default te voldoen.

Continu proces

Let op: dat u de DPIA misschien gaandeweg moet aanpassen, is geen argument om de DPIA uit te stellen of achterwege te laten. Een DPIA uitvoeren is geen eenmalige opdracht, maar een continu proces. U zult altijd moeten (blijven) monitoren of uw gegevensverwerking wijzigt en of u daarom de DPIA moet bijstellen.

Wie moet een DPIA uitvoeren?

Op welke manier moet ik een DPIA uitvoeren?

Moet ik de DPIA publiceren?

Wanneer is een voorafgaande raadpleging nodig?

Functionaris voor de gegevensbescherming (FG)

Per 25 mei 2018 geldt de Algemene verordening gegevensbescherming (AVG). Vanaf dit moment kunnen organisaties verplicht zijn een functionaris voor de gegevensbescherming (FG) aan te stellen. Dit is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG. Op grond van artikel 37 van de AVG is een FG in drie situaties verplicht.

1. **Overheden en publieke organisaties** Ten eerste zijn overheidsinstanties en publieke organisaties altijd verplicht om een FG aan te stellen, ongeacht het type gegevens dat ze verwerken. Het kan gaan om de rijksoverheid, gemeenten en provincies, maar ook om bijvoorbeeld zorg- en onderwijsinstellingen. Voor rechtbanken geldt de verplichte aanstelling van een FG niet.
2. **Observatie** Ten tweede geldt de verplichting om een FG aan te stellen voor organisaties die vanuit hun kernactiviteiten op grote schaal individuen volgen. Het kan hierbij gaan om bijvoorbeeld profilering van mensen voor het maken van risico-inschattingen, cameratoezicht en monitoring van iemands gezondheid via wearables. Relevant hierbij zijn onder meer het aantal mensen dat een organisatie volgt, de hoeveelheid gegevens die deze organisatie verwerkt en hoe lang de organisatie mensen volgt.
3. **Bijzondere persoonsgegevens** Ten derde zijn organisaties verplicht een FG te benoemen als ze op grote schaal bijzondere persoonsgegevens verwerken en dit een kernactiviteit is. Bijzondere persoonsgegevens zijn bijvoorbeeld gegevens over iemands gezondheid, ras, politieke opvatting, geloofsovertuiging of strafrechtelijke verleden.

Andere situaties

EU-lidstaten kunnen ook andere situaties benoemen waarin een FG verplicht is. Het is nog niet bekend of dit in Nederland gaat gebeuren. Wanneer onduidelijk is of u verplicht bent om een FG aan te stellen, moet u goed kunnen onderbouwen waarom u ervoor gekozen hebt om dat wel of niet te doen.

Guidelines FG

De Europese privacytoezichthouders hebben in april 2017 de (definitieve) Guidelines on Data Protection Officers gepubliceerd die meer uitleg geven over de FG. Er is ook een officiële Nederlandse vertaling van de guidelines FG beschikbaar.

VIII. AVG - Wet- en regelgeving

Algemene Verordening Gegevensbescherming (AVG)

VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016

betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)

(Voor de EER relevante tekst)

Weergegeven delen van de AVG:

Hoofdstuk 1 t/m Hoofdstuk 5, zijnde Artikel 1 t/m Artikel 50.

Hoofdstuk 1: Algemene bepalingen

Art. 1: Onderwerp en doelstellingen

1. Bij deze verordening worden regels vastgesteld betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van persoonsgegevens.
2. Deze verordening beschermt de grondrechten en de fundamentele vrijheden van natuurlijke personen en met name hun recht op bescherming van persoonsgegevens.
3. Het vrije verkeer van persoonsgegevens in de Unie wordt noch beperkt noch verboden om redenen die verband houden met de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens.

Art. 2: Materieel toepassingsgebied

1. Deze verordening is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
2. Deze verordening is niet van toepassing op de verwerking van persoonsgegevens:

- a) in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen;

- b) door de lidstaten bij de uitvoering van activiteiten die binnen de werkingssfeer van titel V, hoofdstuk 2, VEU vallen;

- c) door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit;
- d)door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

1. Op de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie is Verordening (EG) nr. 45/2001 van toepassing. Verordening (EG) nr. 45/2001 en andere rechtshandelingen van de Unie die van toepassing zijn op een dergelijke verwerking van persoonsgegevens worden overeenkomstig artikel 98 aan de beginselen en regels van de onderhavige verordening aangepast.
2. Deze verordening laat de toepassing van Richtlijn 2000/31/EG, en met name van de regels in de artikelen 12 tot en met 15 van die richtlijn betreffende de aansprakelijkheid van als tussenpersoon optredende dienstverleners onverlet.

Art. 3 Territoriaal toepassingsgebied

1. Deze verordening is van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Unie, ongeacht of de verwerking in de Unie al dan niet plaatsvindt.

2. Deze verordening is van toepassing op de verwerking van persoonsgegevens van betrokkenen die zich in de Unie bevinden, door een niet in de Unie gevestigde verwerkingsverantwoordelijke of verwerker, wanneer de verwerking verband houdt met:
a) het aanbieden van goederen of diensten aan deze betrokkenen in de Unie, ongeacht of een betaling door de betrokkenen is vereist; of
b) het monitoren van hun gedrag, voor zover dit gedrag in de Unie plaatsvindt.

3. Deze verordening is van toepassing op de verwerking van persoonsgegevens door een verwerkingsverantwoordelijke die niet in de Unie is gevestigd, maar op een plaats waar krachtens het internationaal publiekrecht het lidstatelijke recht van toepassing is.

Art. 4 Definities

1) „persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

2) „verwerking": een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

3) „beperken van de verwerking": het markeren van opgeslagen persoonsgegevens met als doel de verwerking ervan in de toekomst te beperken;

4) „profilering": elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen;

5) „pseudonimisering": het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld;

6) „bestand": elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;

7) „verwerkingsverantwoordelijke": een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoons gegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;

8) „verwerker": een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;

9) „ontvanger": een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk 4.5.2016 L 119/33 Publicatieblad van de Europese Unie NL persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidsta telijke recht gelden echter niet als ontvangers; de verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn;

10) „derde": een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken;

11) „toestemming" van de betrokkene: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt;

12) „inbreuk in verband met persoonsgegevens": een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;

13) „genetische gegevens": persoonsgegevens die verband houden met de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon;

14) „biometrische gegevens": persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens;

15) „gegevens over gezondheid": persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven;

16) „hoofdvestiging":
a) met betrekking tot een verwerkingsverantwoordelijke die vestigingen heeft in meer dan één lidstaat, de plaats waar zijn centrale administratie in de Unie is gelegen, tenzij de beslissingen over de doelstellingen van en de middelen voor de verwerking van persoonsgegevens worden genomen in een andere vestiging van de verwerkingsverantwoordelijke die zich eveneens in de Unie bevindt, en die tevens gemachtigd is die beslissingen uit te voeren, in welk geval de vestiging waar die beslissingen worden genomen als de hoofdvestiging wordt beschouwd;

b) met betrekking tot een verwerker die vestigingen in meer dan één lidstaat heeft, de plaats waar zijn centrale administratie in de Unie is gelegen of, wanneer de verwerker geen centrale administratie in de Unie heeft, de vestiging van de verwerker in de Unie waar de voornaamste verwerkingsactiviteiten in het kader van de activiteiten van een vestiging van de verwerker plaatsvinden, voor zover op de verwerker krachtens deze verordening specifieke verplichtingen rusten;

17) „vertegenwoordiger": een in de Unie gevestigde natuurlijke persoon of rechtspersoon die uit hoofde van artikel 27 schriftelijk door de verwerkingsverantwoordelijke of de verwerker is aangewezen om de verwerkingsverantwoordelijke of de verwerker te vertegenwoordigen in verband met hun respectieve verplichtingen krachtens deze verordening;

18) „onderneming": een natuurlijke persoon of rechtspersoon die een economische activiteit uitoefent, ongeacht de rechtsvorm ervan, met inbegrip van maatschappen en persoonsvennootschappen of verenigingen die regelmatig een economische activiteit uitoefenen;

19) „concern": een onderneming die zeggenschap uitoefent en de ondernemingen waarover die zeggenschap wordt uitgeoefend;

20) „bindende bedrijfsvoorschriften": beleid inzake de bescherming van persoonsgegevens dat een op het grondgebied van een lidstaat gevestigde verwerkingsverantwoordelijke of verwerker voert met betrekking tot de doorgifte of reeksen van doorgiften van persoonsgegevens aan een verwerkingsverantwoordelijke of verwerker in een of meerderde landen binnen een concern of een groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen;

21) „toezichthoudende autoriteit": een door een lidstaat ingevolge artikel 51 ingestelde onafhankelijke overheidsinstantie;

22) „betrokken toezichthoudende autoriteit": een toezichthoudende autoriteit die betrokken is bij de

verwerking van persoonsgegevens omdat:

a) de verwerkingsverantwoordelijke of de verwerker op het grondgebied van de lidstaat van die toezichthoudende autoriteit is gevestigd;
b) de betrokkenen die in de lidstaat van die toezichthoudende autoriteit verblijven, door de verwerking wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden; of
d) bij die toezichthoudende autoriteit een klacht is ingediend;
e)
23) „grensoverschrijdende verwerking":

a) verwerking van persoonsgegevens in het kader van de activiteiten van vestigingen in meer dan één lidstaat van een verwerkingsverantwoordelijke of een verwerker in de Unie die in meer dan één lidstaat is gevestigd; of b) verwerking van persoonsgegevens in het kader van de activiteiten van één vestiging van een verwerkingsverantwoordelijke of van een verwerker in de Unie, waardoor in meer dan één lidstaat betrokkenen wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden; 24) „relevant en gemotiveerd bezwaar": een bezwaar tegen een ontwerpbesluit over het bestaan van een inbreuk op deze verordening of over de vraag of de voorgenomen maatregel met betrekking tot de verwerkingsverantwoordelijke of de verwerker strookt met deze verordening, waarin duidelijk de omvang wordt aangetoond van de risico's die het ontwerpbesluit inhoudt voor de grondrechten en de fundamentele vrijheden van betrokkenen en, indien van toepassing, voor het vrije verkeer van persoonsgegevens binnen de Unie;25) „dienst van de informatiemaatschappij": een dienst als gedefinieerd in artikel 1, lid 1, punt b), van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad (1);

26) „internationale organisatie": een organisatie en de daaronder vallende internationaalpubliekrechtelijke organen of andere organen die zijn opgericht bij of op grond van een overeenkomst tussen twee of meer landen.

Hoofdstuk 2: Beginselen

Art. 5 Beginselen inzake verwerking van persoonsgegevens

1. Persoonsgegevens moeten:

a) worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is („rechtmatigheid, behoorlijkheid en transparantie");
b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd („doelbinding");
c) toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt („minimale gegevensverwerking");
d) juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren („juistheid"); (1) Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij (PB L 241 van 17.9.2015, blz. 1).
e) worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en

vrijheden van de betrokkene te beschermen („opslagbeperking");
f) door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging („integriteit en vertrouwelijkheid").

2. De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze aantonen („verantwoordingsplicht").

Art. 6 Rechtmatigheid van de verwerking

1. De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:

a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
b) de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
d) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is. De eerste alinea, punt f), geldt niet voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken.

2. De lidstaten kunnen specifiekere bepalingen handhaven of invoeren ter aanpassing van de manier waarop de regels van deze verordening met betrekking tot de verwerking met het oog op de naleving van lid 1, punten c) en e), worden toegepast; hiertoe kunnen zij een nadere omschrijving geven van specifieke voorschriften voor de verwerking en andere maatregelen om een rechtmatige en behoorlijke verwerking te waarborgen, ook voor andere specifieke verwerkingssituaties als bedoeld in hoofdstuk IX.

1. De rechtsgrond voor de in lid 1, punten c) en e), bedoelde verwerking moet worden vastgesteld bij:
a) Unierecht; of
b) lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is.
Het doel van de verwerking wordt in die rechtsgrond vastgesteld of is met betrekking tot de in lid 1, punt e), bedoelde verwerking noodzakelijk voor de vervulling van een taak van algemeen belang of voor de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend. Die rechtsgrond kan specifieke bepalingen bevatten om de toepassing van de regels van deze verordening aan te passen, met inbegrip van de algemene voorwaarden inzake de rechtmatigheid van verwerking door de verwerkingsverantwoordelijke; de types verwerkte gegevens; de betrokkenen; de entiteiten waaraan en de doeleinden waarvoor de persoonsgegevens mogen worden verstrekt; de doelbinding; de opslag perioden; en de verwerkingsactiviteiten en -procedures, waaronder maatregelen om te zorgen voor een rechtmatige en behoorlijke verwerking, zoals die voor andere specifieke verwerkingssituaties als bedoeld in hoofdstuk IX. Het Unierecht of het lidstatelijke recht moet beantwoorden aan een doelstelling van algemeen belang en moet evenredig zijn met het nagestreefde gerechtvaardigde doel.

4. Wanneer de verwerking voor een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld

niet berust op toestemming van de betrokkene of op een Unierechtelijke bepaling of een lidstaatrechtelijke bepaling die in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborging van de in artikel 23, lid 1, bedoelde doelstellingen houdt de verwerkingsverantwoordelijke bij de beoordeling van de vraag of de verwerking voor een ander doel verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld onder meer rekening met:

a) ieder verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld, en de doeleinden van de voorgenomen verdere verwerking;
b) het kader waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkenen en de verwerkingsverantwoordelijke betreft;
c) de aard van de persoonsgegevens, met name of bijzondere categorieën van persoonsgegevens worden verwerkt, overeenkomstig artikel 9, en of persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten worden verwerkt, overeenkomstig artikel 10;
d) de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkenen;
e) het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering.

Art. 7 Voorwaarden voor toestemming

1. Wanneer de verwerking berust op toestemming, moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens.

2. Indien de betrokkene toestemming geeft in het kader van een schriftelijke verklaring die ook op andere aangelegenheden betrekking heeft, wordt het verzoek om toestemming in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal zodanig gepresenteerd dat een duidelijk onderscheid kan worden gemaakt met de andere aangelegenheden. Wanneer een gedeelte van een dergelijke verklaring een inbreuk vormt op deze verordening, is dit gedeelte niet bindend.

3. De betrokkene heeft het recht zijn toestemming te allen tijde in te trekken. Het intrekken van de toestemming laat de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan, onverlet. Alvorens de betrokkene zijn toestemming geeft, wordt hij daarvan in kennis gesteld. Het intrekken van de toestemming is even eenvoudig als het geven ervan.

4. Bij de beoordeling van de vraag of de toestemming vrijelijk kan worden gegeven, wordt onder meer ten sterkste rekening gehouden met de vraag of voor de uitvoering van een overeenkomst, met inbegrip van een dienstenovereenkomst, toestemming vereist is voor een verwerking van persoonsgegevens die niet noodzakelijk is voor de uitvoering van die overeenkomst.

Art. 8 Voorwaarden voor de toestemming van kinderen met betrekking tot diensten van de informatiemaatschappij

1. Wanneer artikel 6, lid 1, punt a), van toepassing is in verband met een rechtstreeks aanbod van diensten van de informatiemaatschappij aan een kind, is de verwerking van persoonsgegevens van een kind rechtmatig wanneer het kind ten minste 16 jaar is. Wanneer het kind jonger is dan 16 jaar is zulke verwerking slechts rechtmatig indien en voor zover de toestemming of machtiging tot toestemming in dit verband wordt verleend door de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt. De lidstaten kunnen dienaangaande bij wet voorzien in een lagere leeftijd, op voorwaarde dat die leeftijd niet onder 13 jaar ligt.

2. Met inachtneming van de beschikbare technologie doet de verwerkingsverantwoordelijke redelijke inspanningen om in dergelijke gevallen te controleren of de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt, toestemming heeft gegeven of machtiging tot toestemming heeft verleend.

3. Lid 1 laat het algemene overeenkomstenrecht van de lidstaten, zoals de regels inzake de geldigheid, de totstandkoming of de gevolgen van overeenkomsten ten opzichte van kinderen, onverlet.

Art. 9 Verwerking van bijzondere categorieën van persoonsgegevens

Art. 10 Verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten

Art. 11 Verwerking waarvoor identificatie niet is vereist

Hoofdstuk 3: Rechten van de betrokkene

Afd. 1 Transparantie en regelingen

Art. 12 Transparante informatie, communicatie en nadere regels voor de uitoefening van de rechten van de betrokkene

1. De verwerkingsverantwoordelijke neemt passende maatregelen opdat de betrokkene de in de artikelen 13 en 14 bedoelde informatie en de in de artikelen 15 tot en met 22 en artikel 34 bedoelde communicatie in verband met de verwerking in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal ontvangt, in het bijzonder wanneer de informatie specifiek voor een kind bestemd is. De informatie wordt schriftelijk of met andere middelen, met inbegrip van, indien dit passend is, elektronische middelen, verstrekt. Indien de betrokkene daarom verzoekt, kan de informatie mondeling worden meegedeeld, op voorwaarde dat de identiteit van de betrokkene met andere middelen bewezen is.

2. De verwerkingsverantwoordelijke faciliteert de uitoefening van de rechten van de betrokkene uit hoofde van de artikelen 15 tot en met 22. In de in artikel 11, lid 2, bedoelde gevallen mag de verwerkingsverantwoordelijke niet weigeren gevolg te geven aan het verzoek van de betrokkene om diens rechten uit hoofde van de artikelen 15 tot en met 22 uit te oefenen, tenzij de verwerkingsverantwoordelijke aantoont dat hij niet in staat is de betrokkene te identificeren.

3. De verwerkingsverantwoordelijke verstrekt de betrokkene onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek krachtens de artikelen 15 tot en met 22 informatie over het gevolg dat aan het verzoek is gegeven. Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. De verwerkingsverantwoordelijke stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van een dergelijke verlenging. Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt.

4. Wanneer de verwerkingsverantwoordelijke geen gevolg geeft aan het verzoek van de betrokkene, deelt hij deze laatste onverwijld en uiterlijk binnen één maand na ontvangst van het verzoek mee waarom het verzoek zonder gevolg is gebleven, en informeert hij hem over de mogelijkheid om klacht in te dienen bij een toezichthoudende autoriteit en beroep bij de rechter in te stellen.

5. Het verstrekken van de in de artikelen 13 en 14 bedoelde informatie, en het verstrekken van de communicatie en het treffen van de maatregelen bedoeld in de artikelen 15 tot en met 22 en artikel 34 geschieden kosteloos. Wanneer verzoeken van een betrokkene kennelijk ongegrond of buitensporig zijn, met name vanwege hun repetitieve karakter, mag de verwerkingsverantwoordelijke ofwel:
a) een redelijke vergoeding aanrekenen in het licht van de administratieve kosten waarmee het verstrekken van de gevraagde informatie of communicatie en het treffen van de gevraagde maatregelen gepaard gaan; ofwel
b) weigeren gevolg te geven aan het verzoek.

Het is aan de verwerkingsverantwoordelijke om de kennelijk ongegronde of buitensporige aard van het verzoek aan te tonen.

6. Onverminderd artikel 11 kan de verwerkingsverantwoordelijke, wanneer hij redenen heeft om te twijfelen aan de identiteit van de natuurlijke persoon die het verzoek indient als bedoeld in de artikelen 15 tot en met 21, om aanvullende informatie vragen die nodig is ter bevestiging van de identiteit van de betrokkene.

7. De krachtens de artikelen 13 en 14 aan betrokkenen te verstrekken informatie mag worden verstrekt met gebruikmaking van gestandaardiseerde iconen, om de betrokkene een nuttig overzicht, in een goed zichtbare, begrijpelijke en duidelijk leesbare vorm, van de voorgenomen verwerking te bieden. Wanneer de iconen elektronisch worden weergegeven, zijn ze machine leesbaar.

8. De Commissie is bevoegd overeenkomstig artikel 92 gedelegeerde handelingen vast te stellen om te bepalen welke informatie de iconen dienen weer te geven en via welke procedures de gestandaardiseerde iconen tot stand dienen te komen.

Afd. 2 Informatie en toegang tot persoonsgegevens

Art. 13 Te verstrekken informatie wanneer persoonsgegevens bij de betrokkene worden verzameld

Art. 14 Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen

Art. 15 Recht van inzage van de betrokkene

1. De betrokkene heeft het recht om van de verwerkingsverantwoordelijke uitsluitsel te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen van die persoonsgegevens en van de volgende informatie:
a) de verwerkingsdoeleinden;
b) de betrokken categorieën van persoonsgegevens;
c) de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties;
d) indien mogelijk, de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
e) dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken dat persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van hem betreffende persoonsgegevens wordt beperkt, alsmede het recht tegen die verwerking bezwaar te maken;
f) dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;
g) wanneer de persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens;
h) het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4, bedoelde profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

2. Wanneer persoonsgegevens worden doorgegeven aan een derde land of een internationale organisatie, heeft de betrokkene het recht in kennis te worden gesteld van de passende waarborgen overeenkomstig artikel 46 inzake de doorgifte.

3. De verwerkingsverantwoordelijke verstrekt de betrokkene een kopie van de persoonsgegevens die worden verwerkt. Indien de betrokkene om bijkomende kopieën verzoekt, kan de verwerkingsverantwoordelijke op basis van de administratieve kosten een redelijke vergoeding aanrekenen. Wanneer de betrokkene zijn verzoek elektronisch indient, en niet om een andere regeling verzoekt, wordt de informatie in een gangbare elektronische vorm verstrekt.

4. Het in lid 3 bedoelde recht om een kopie te verkrijgen, doet geen afbreuk aan de rechten en vrijheden van anderen.

Afd. 3 Rectificatie en wissing van gegevens

Art. 16 Recht op rectificatie

De betrokkene heeft het recht om van de verwerkingsverantwoordelijke onverwijld rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen. Met inachtneming van de doeleinden van de verwerking heeft de betrokkene het recht vervollediging van onvolledige persoonsgegevens te verkrijgen, onder meer door een aanvullende verklaring te verstrekken.

Art. 17 Recht op gegevenswissing („recht op vergetelheid")

1. De betrokkene heeft het recht van de verwerkingsverantwoordelijke zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen en de verwerkingsverantwoordelijke is verplicht persoonsgegevens zonder onredelijke vertraging te wissen wanneer een van de volgende gevallen van toepassing is:
a) de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt; 4.5.2016 L 119/43 Publicatieblad van de Europese Unie NL
b) de betrokkene trekt de toestemming waarop de verwerking overeenkomstig artikel 6, lid 1, punt a), of artikel 9, lid 2, punt a), berust, in, en er is geen andere rechtsgrond voor de verwerking;
c) de betrokkene maakt overeenkomstig artikel 21, lid 1, bezwaar tegen de verwerking, en er zijn geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking, of de betrokkene maakt bezwaar tegen de verwerking overeenkomstig artikel 21, lid 2;
d) de persoonsgegevens zijn onrechtmatig verwerkt;
e) de persoonsgegevens moeten worden gewist om te voldoen aan een in het Unierecht of het lidstatelijke recht neergelegde wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
f) de persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij als bedoeld in artikel 8, lid 1.

2. Wanneer de verwerkingsverantwoordelijke de persoonsgegevens openbaar heeft gemaakt en overeenkomstig lid 1 verplicht is de persoonsgegevens te wissen, neemt hij, rekening houdend met de beschikbare technologie en de uitvoeringskosten, redelijke maatregelen, waaronder technische maatregelen, om verwerkingsverantwoordelijken die de persoonsgegevens verwerken, ervan op de hoogte te stellen dat de betrokkene de verwerkingsverantwoordelijken heeft verzocht om iedere koppeling naar, of kopie of reproductie van die persoonsgegevens te wissen.

3. De leden 1 en 2 zijn niet van toepassing voor zover verwerking nodig is:
a) voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie;
b) voor het nakomen van een in een het Unierecht of het lidstatelijke recht neergelegde wettelijke verwerkingsverplichting die op de verwerkingsverantwoordelijke rust, of voor het vervullen van een taak van algemeen belang of het uitoefenen van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend;
c) om redenen van algemeen belang op het gebied van volksgezondheid overeenkomstig artikel 9, lid 2, punten h) en i), en artikel 9, lid 3;
d) met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89, lid 1, voor zover het in lid 1 bedoelde recht de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen;
e)voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

Art. 18 Recht op beperking van de verwerking

1. De betrokkene heeft het recht van de verwerkingsverantwoordelijke de beperking van de verwerking te verkrijgen indien een van de volgende elementen van toepassing is:
a) de juistheid van de persoonsgegevens wordt betwist door de betrokkene, gedurende een periode die de verwerkingsverantwoordelijke in staat stelt de juistheid van de persoonsgegevens te controleren;
b) de verwerking is onrechtmatig en de betrokkene verzet zich tegen het wissen van de persoonsgegevens en verzoekt in de plaats daarvan om beperking van het gebruik ervan;
c) de verwerkingsverantwoordelijke heeft de persoonsgegevens niet meer nodig voor de verwerkingsdoeleinden, maar de betrokkene heeft deze nodig voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
d) de betrokkene heeft overeenkomstig artikel 21, lid 1, bezwaar gemaakt tegen de verwerking, in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van de verwerkingsverantwoordelijke zwaarder wegen dan die van de betrokkene.

2. Wanneer de verwerking op grond van lid 1 is beperkt, worden persoonsgegevens, met uitzondering van de opslag ervan, slechts verwerkt met toestemming van de betrokkene of voor de instelling, uitoefening of onderbouwing van een rechtsvordering of ter bescherming van de rechten van een andere natuurlijke persoon of rechtspersoon of om gewichtige redenen van algemeen belang voor de Unie of voor een lidstaat.

3. Een betrokkene die overeenkomstig lid 1 een beperking van de verwerking heeft verkregen, wordt door de verwerkingsverantwoordelijke op de hoogte gebracht voordat de beperking van de verwerking wordt opgeheven.

Art. 19 Kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens of verwerkingsbeperking

Art. 20 Recht op overdraagbaarheid van gegevens

Afd. 4 Recht van bezwaar en geautomatiseerde individuele besluitvorming

Art. 21 Recht van bezwaar

Art. 22 Geautomatiseerde individuele besluitvorming, waaronder profilering

Afd. 5 Beperkingen

Art. 23 Beperkingen

Hoofdstuk 4: Verwerkingsverantwoordelijke en verwerker

Afd. 1 Algemene verplichtingen

Art. 24 Verantwoordelijkheid van de verwerkingsverantwoordelijke

1. Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.

2. Wanneer zulks in verhouding staat tot de verwerkingsactiviteiten, omvatten de in lid 1 bedoelde maatregelen een passend gegevensbeschermingsbeleid dat door de verwerkingsverantwoordelijke wordt uitgevoerd.
3. Het aansluiten bij goedgekeurde gedragscodes als bedoeld in artikel 40 of goedgekeurde certificeringsmechanismen als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat de verplichtingen van de verwerkingsverantwoordelijke zijn nagekomen.

Art. 25 Gegevensbescherming door ontwerp en door standaardinstellingen

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden, treft de verwerkingsverantwoordelijke, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, zoals pseudonimisering, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen.

2. De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan. Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.

3. Een overeenkomstig artikel 42 goedgekeurd certificeringsmechanisme kan worden gebruikt als element om aan te tonen dat aan de voorschriften van de leden 1 en 2 van dit artikel is voldaan.

Art. 26 Gezamenlijke verwerkingsverantwoordelijken

1. Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken. Zij stellen op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van deze verordening vast, met name met betrekking tot de uitoefening van de rechten van de betrokkene en hun respectieve verplichtingen om de in de artikelen 13 en 14 bedoelde informatie te verstrekken, door middel van een onderlinge regeling, tenzij en voor zover de respectieve verantwoordelijkheden van de verwerkingsverantwoordelijken zijn vastgesteld bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijken van toepassing is. In de regeling kan een contactpunt voor betrokkenen worden aangewezen.

2. Uit de in lid 1 bedoelde regeling blijkt duidelijk welke rol de gezamenlijke verwerkingsverantwoordelijken respectievelijk vervullen, en wat hun respectieve verhouding met de betrokkenen is. De wezenlijke inhoud van de regeling wordt aan de betrokkene beschikbaar gesteld.

3. Ongeacht de voorwaarden van de in lid 1 bedoelde regeling, kan de betrokkene zijn rechten uit hoofde van deze verordening met betrekking tot en jegens iedere verwerkingsverantwoordelijke uitoefenen.

Art. 27 Vertegenwoordigers van niet in de Unie gevestigde verwerkingsverantwoordelijken of verwerkers

Art. 28 Verwerker

Hoofdstuk 5: Doorgiften van persoonsgegevens aan derde landen of internationale organisaties

Art. 48 Niet bij Unierecht toegestane doorgiften of verstrekkingen

Art. 49 Afwijkingen voor specifieke situaties

Art. 50 Internationale samenwerking voor de bescherming van persoonsgegevens